BRIAN KREBS

# NAȚIUNEA SPAM

Din culisele criminalității informatice

CORINT FUTURE

„În ciuda îngrijorării guvernelor, reacţia factorilor de decizie la nivel înalt faţă de mecanismele organizaţionale şi tehnologice care alimentează epidemia de spam a fost apatică în cel mai fericit caz, iar, pe alocuri, practic inexistentă. Deşi avem de a face cu o ameninţare capabilă să perturbe funcţionarea infrastructurii unor ţări întregi, să blocheze reţele de comunicaţii vitale, să intoxice populaţia prin răspândirea unor bunuri de consum contrafăcute şi să stimuleze dezvoltarea unei economii ilegale, guvernele din întreaga lume n-au făcut mare lucru pentru a-şi proteja cetăţenii de aceste armate informatice invadatoare."

BRIAN KREBS

BRIAN KREBS

# NAȚIUNEA SPAM

CORINT FUTURE

Colecţie coordonată de
ADA ROSETI

BRIAN KREBS

# NAȚIUNEA SPAM

## Din culisele criminalității informatice

Traducere din limba engleză
DAN DRUMUR

Prefață
EUGEN GLĂVAN

CORINT BOOKS
2019

**Lectură de specialitate:** Liviu Pop
**Redactare și glosar:** Dan Criste
**Tehnoredactare:** Mihaela Ciufu
**Design copertă:** Dan Mihalache
**Ilustrația copertei:** © Shutterstock

BRIAN KREBS
*Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door*
Copyright © 2014 by Brian Krebs
Originally published in the United States by Sourcebook, Inc.
All rights reserved.

Toate drepturile asupra ediției în limba română aparțin
EDITURII CORINT BOOKS.

ISBN: 978-606-793-602-5

Descrierea CIP a Bibliotecii Naționale a României
KREBS, BRIAN
Națiunea Spam: din culisele criminalității informatice / Brian Krebs; trad. din lb. engleză de Dan Drumur; pref. de Eugen Glăvan.
București: Corint Books, 2019

ISBN 978-606-793-602-5

I. Drumur, Dan (trad.)
II. Glăvan, Eugen (pref.)

004

# PREFAȚĂ

Fiecare epocă istorică are drept principală caracteristică mijlocul tehnologic dominant de comunicare și fiecare societate s-a clădit pe capacitatea de a produce cunoaștere. Capacitatea de a transmite informații populației și generațiilor viitoare a fundamentat constituirea civilizațiilor, iar manuscrisele care limitau cunoașterea la un cerc de inițiați au reprezentat primele forme de control al informației. Tiparul a generalizat accesul și a pus bazele alfabetizării. Fotografia a fixat imaginea, iar telefonul și radioul au purtat pe unde cuvântul și muzica. Televiziunea a integrat cuvântul, imaginea și sunetul, devenind mijlocul de comunicare specific în societățile moderne.

În prezent, internetul reprezintă modalitatea informațională și comunicațională predominantă la scară planetară, înglobând interacțiunea mediată în timp real. Toate aceste tehnologii au avut nevoie de timp pentru a fi acceptate în societate și au produs schimbări majore. Fiecare a generat câștigători și perdanți, legi și fărădelegi, eroi și tâlhari. Este momentul să facem cunoștință cu un aspect negativ al internetului, trimiterea de mesaje electronice nesolicitate sau spamul, care, în 2013, reprezenta 70% din volumul total de e-mailuri expediate zilnic.

*Națiunea Spam* este povestea unor personaje dubioase care, într-o societate permisivă și lipsită de capacitatea și

interesul de a impune legea, au elaborat planuri sofisticate de fraudare bazate pe e-mailurile nesolicitate. Bazându-se pe slăbiciunile sistemelor de operare ale computerelor, încălcând legi naționale sau exploatând zone insuficient de bine definite ale criminalității transfrontaliere, acești hoți informatici au creat programe informatice specializate, care, prin infectarea computerelor și preluarea controlului acestora, se constituie în botneturi. Controlate de spammeri, acestea trimit reclame nesolicitate prin intermediul mesajelor electronice.

Citind această carte, vom face cunoștință cu Pavel „RedEye" Vrublevski, lăudărosul și instabilul artizan al ChronoPay și Rx-Promotion, și competitorii acestuia, Igor „Desp" Gusev și Dmitri „SaintD" Stupin, creatorii SpamIt și GlavMed. În momentul scrierii volumului de față, acesta era cel mai mare program farmaceutic ilicit on-line de pe planetă. Miza concurenței dintre ei o reprezintă controlul asupra unei industrii rentabile, de sute de milioane de dolari, care intermediază vânzarea de medicamente ce necesită rețetă. Angrenate în dispută sunt organizații antispam, firme de plăți on-line, companii medicale și servicii de securitate. Fundalul este societatea rusă incapabilă să impună aplicarea legilor, măcinată de corupție, dezinteresată de activitățile infracționale care aduc pagube cetățenilor și instituțiilor străine.

Autorul cărții, Brian Krebs, este un jurnalist american de investigații, reporter, între 1995 și 2009, la ziarul *Washington Post*. Fiind specializat în criminalitatea informatică și securitatea computerelor, el identifica și demasca, în articolele publicate pe această temă, o serie de activități ilicite care exploatau slăbiciunile internetului pentru profit. Constatând că abordarea jurnalistică clasică față de fraudele cibernetice nu este adecvată, acesta demisionează și creează propriul blog de investigații în domeniul securității pe internet, KrebsOnSecurity.com. Un indicator relevant al profesionalismului lui Brian Krebs este faptul că, în 2016, după publicarea

cărții, blogul său a fost ținta celui mai mare atac DDoS până la data respectivă.

Apărut în 2014, volumul de față se referă la un episod specific, definit în timp al constantului război dintre autorități, companii, organizațiile de securitate cibernetică și infractori, care se rezumă la controlul informației pe internet. E-mailurile nesolicitate sunt create de către hackeri și conțin oferte de produse cum ar fi medicamente, pornografie, materiale piratate. Subiectul principal al cărții este reprezentat de apariția farmaciilor on-line ilicite și a rețelelor din spatele acestora, de la creatorii de malware până la consumatorul final. Prima observație pe care trebuie să o facem este aceea că, deși scrisă într-un ritm alert și având aerul unei povești neverosimile, cartea nu este una de ficțiune sau speculativă. Prezentarea subiectului este rezultatul unei investigații jurnalistice riguroase, în care autorul citează surse, discută cu martori, studiază baze de date și face apel la experți. Al doilea aspect se referă la accesibilitate. Deși abordează o temă complexă din punct de vedere tehnologic și dificilă, la prima vedere, din punct de vedere conceptual și terminologic, cartea se citește ușor și nu necesită cunoștințe de specialitate avansate.

Scopul volumului de față este acela de a informa și de a educa. El prezintă practici ilegale, care profită de disfuncționalități din societate, precum și modalitățile specifice în care infractorii extrag informații. Cititorii pot afla care sunt cele mai bune metode pe care le pot folosi pentru a se proteja. Comportamentul on-line și consecințele acestuia presupun o atitudine activă, nu doar cunoștințe tehnice și actualizări ale programelor informatice, dar și evitarea informațiilor din surse nesigure și accesarea linkurilor dubioase.

Relevanța cărții pentru România este indirectă și privește modul în care societatea românească poate gravita spre componenta infracțională sau spre cea a luptei contra practicilor ilicite. În material, sunt amintite vag rețele infracționale

localizate în estul Europei. Obținerea unor medicamente în România este foarte dificilă, deoarece legislația este imprecisă și instabilă, iar importul este uneori subvenționat. Nu e de mirare că se caută soluții pentru livrarea lor discretă și accesibilă, iar oferta spammerilor se încadrează în această categorie. Mass-media a relatat cazuri de rețele informale care facilitează importul și distribuirea de medicamente, evitând canalele aprobate oficial.

Finalul cărții oferă o imagine dublă și un avertisment. „Războiul farmaceutic" și implicarea autorităților au dus la scăderea globală a spamului. Contextul infracțional cibernetic din Rusia poate servi însă intereselor statului, așa cum se va dovedi după publicarea cărții. Experiența răufăcătorilor cibernetici privați este transformată în programe de subminare a statelor democratice și de finanțare a unor armate de troli pentru a semăna discordie. Infractorii se orientează spre informațiile personale și rețelele sociale, beneficiind de neinformarea și apatia utilizatorilor.

EUGEN GLĂVAN

# NOTĂ ASUPRA EDIȚIEI ÎN LIMBA ROMÂNĂ

Pentru ușurarea lecturii, am ales să ignorăm unele reguli de ortografiere a cuvintelor străine neintrate încă sau intrate de puțin timp în vocabularul limbii române, majoritatea lor făcând parte din limbajul specific domeniului tratat în lucrare. Astfel, nu s-a mai folosit cratima la formele de plural sau articulate ale unor substantive precum *spammer* (*spammer*-i, *spammer*-ul), *malware* (*malware*-ul), *botnet* (*botnet*-uri, *botnet*-ul) etc., optându-se pentru variantele „spammeri", „spammerul", „malwareul", respectiv „botneturi", „botnetul". De altfel, unele noțiuni, precum „e-mail", „soft", „spam", au intrat deja în vocabularul de la noi, ortografiindu-se, la formele menționate mai înainte, „e-mailuri", „e-mailul", „softuri", „softul", respectiv „spamuri", „spamul". De asemenea, în scrierea majorității cuvintelor de origine străină, nu s-au folosit caracterele cursive.

La finalul cărții, am inclus un glosar de termeni menit să-l ajute pe cititor să înțeleagă unele concepte specifice subiectului abordat. În el am introdus, pe lângă noțiuni din sfera informaticii, câteva expresii din domeniul financiar-bancar.

*Editura*

*Pentru BizMgr a mea*

# PERSONAJE CELEBRE DIN CIBERSPAȚIU

**PAVEL VRUBLEVSKI**, pseudonim „RedEye" – cofondator al companiei ChronoPay, furnizor de servicii de plată și procesare a cardurilor de mare risc, puternic asociat cu industria antivirușilor dubioși. Cofondator al programului de afiliere a farmaciilor Rx-Promotion.

**IURI KABAIENKOV**, pseudonim „Hellman" – proprietar, împreună cu Pavel Vrublevski, al Rx-Promotion.

**IGOR GUSEV**, pseudonim „Desp" – cofondator al ChronoPay și coproprietar al parteneriatelor de spam farmaceutic SpamIt și GlavMed.

**DMITRI STUPIN** – proprietar, împreună cu Igor Gusev, al parteneriatelor de spam farmaceutic SpamIt și GlavMed.

**IGOR VIȘNEVSKI** – spammer care a ajutat la crearea botnetului de spam Cutwail și a fost partener de afaceri al faimosului spammer Dmitri „Gugle" Necivolod.

**DMITRI NECIVOLOD**, pseudonim „Gugle" – unul dintre cei mai prosperi spammeri ai SpamIt și Rx-Promotion, care și-a închiriat botnetul de spam Cutwail pentru a fi folosit de mulți alți spammeri.

**GHENNADI LOGHINOV** – cetățean belarus și lider al grupării militante de crimă organizată „Satul". Partener cu Aleksandr Rubațki, implicat în răpirea și răscumpărarea afaceristului rival Evgheni „Pet" Petrovski.

**ALEKSANDR RUBAȚKI** – hacker din Belarus. A avut legături strânse cu industria pornografică infantilă și a înființat ulterior, la Sankt Petersburg, Russian Business Network (RBN).

**EVGHENI PETROVSKI**, pseudonim „Pet" – proprietar belarus al companiilor Sunbill și BillCards, rețele de procesare a cardurilor de credit implicate în sistemul de plăți pentru siteurile de pornografie infantilă.

**NIKOLAI MCCOLO**, pseudonim „Kolea" – tânăr întreprinzător aflat în spatele companiei McColo Corp., care, până la dispariția ei în 2008, a fost unul dintre cei mai populari furnizori de găzduire web din domeniul criminalității informatice.

**LEONID KUVAIEV** – spammer condamnat, care a gestionat programul de spam farmaceutic RxPartners. În prezent, Kuvaiev execută o pedeapsă de zece ani de închisoare în Rusia pentru abuz și pornografie infantilă.

**IGOR** și **DMITRI ARTIMOVICI**, pseudonim „Engel" – frați care se pare că ar fi operat botnetul de spam Festi și au fost apropiați de Vrublevski. În 2013, frații Artimovici au fost condamnați pentru utilizarea lui Festi în vederea atacării siteului Assist, un concurent al ChronoPay, deși ei au negat acuzația respectivă.

**COSMA** – spammer atât pentru GlavMed–SpamIt, cât și pentru Rx-Promotion, și creator principal al botnetului Rustock.

**SEVERA** – spammer atât pentru GlavMed–SpamIt, cât și pentru Rx-Promotion; presupusul creator al botneturilor Waledac și Storm.

# Capitolul 1

# PARAZIT

BMW-ul 760 bleumarin s-a oprit la o trecere de pietoni semaforizată din centrul Moscovei. Un Porsche Cayenne negru s-a oprit alături. Era duminică, 2 septembrie 2007, ora 14, iar străzile, în mod obişnuit aglomerate, din apropierea faimoasei Pieţe Suharevskaia erau aproape lipsite de trafic, cu excepţia turiştilor şi a localnicilor care se plimbau pe trotuarele late de pe ambele părţi ale bulevardului. Soarele după-amiezii, care încălzise străzile pe tot parcursul zilei, începea să proiecteze pe stradă umbrele lungi ale clădirilor istorice din apropiere.

Şoferul BMW-ului, un escroc local notoriu, cunoscut ca hacker sub pseudonimul „Jaks", devenise tată în ziua aceea şi, împreună cu pasagerul, băuse o cantitate impresionantă de votcă în cinstea nou-născutului. Era momentul şi locul perfect pentru tranşarea unei rivalităţi mocnite cu şoferul automobilului Porsche: trebuia să afle care dintre maşini e mai rapidă. Ambii şoferi au ambalat motoarele într-o înţelegere nerostită de a se întrece pe distanţa scurtă care-i despărţea de piaţa mare aflată chiar în faţă.

Când s-a aprins lumina verde a semaforului, scârţâiturile produse de cauciucuri pe beton s-au auzit la sute de metri depărtare în Suharevskaia. Pietonii s-au întors să vadă automobilele performante care au ţâşnit din intersecţie unul lângă celălalt şi au atins o viteză ameţitoare.

Trecând cu peste 200 km/h de mijlocul distanței, Jaks a pierdut deodată controlul volanului, a atins cealaltă mașină și a intrat într-un uriaș stâlp metalic de iluminat. Într-o clipă, întrecerea s-a sfârșit fără niciun învingător. BMW-ul era rupt în două, iar Porsche-ul, făcut ferfeniță, ardea mocnit în apropiere. Ambii șoferi s-au îndepărtat șchiopătând de locul accidentului, dar pasagerul din BMW – Nikolai McColo, o tânără speranță a Internetului în vârstă de 23 de ani – a murit pe loc, aproape decapitat, prins sub mașina de lux.

„Kolea", așa cum îi spuneau prietenii, era o mică celebritate în lumea subterană a criminalității informatice, cel mai tânăr angajat al firmei de familie McColo Corp., care furniza servicii de găzduire web. Într-un moment în care autoritățile din toată lumea începeau să-și dea seama de pericolele de ordin financiar și organizațional ale criminalității informatice, McColo Corp. devenise cunoscută drept unul dintre centrele acesteia: un loc în care escrocii de pe internet își puteau începe afacerile fără să se teamă că investițiile și planurile lor on-line vor fi descoperite sau puse în pericol de diverse autorități străine.

În momentul morții lui Kolea, serverele familiei sale găzduiau cele mai mari afaceri din lume implicate în distribuirea de e-mailuri nesolicitate sau „spam" prin intermediul rețelelor automate. Aceste rețele, denumite „botneturi", sunt grupuri de computere personale care au fost piratate și în care a fost instalat software rău intenționat – „malware" – ce le permite atacatorilor să controleze de la distanță sistemele respective. De obicei, proprietarii nu au habar că acele computere sunt controlate de altcineva.

Aproape toate botneturile controlate de McColo erau create pentru a distribui reclamele nedorite care ne umplu zilnic conturile de e-mail și suprasolicită filtrele antispam. Serverele lui McColo nu generau și nu pompau ele însele spam – acest lucru ar fi atras atenția așa-zișilor gardieni ai internetului

și poliției din țările occidentale. Ele erau folosite doar de afacerile botmaster pentru a manipula milioane de computere de pe întreg globul și a le transforma în zombi distribuitori de spam.

În timp ce personalul de pe ambulanță termina de curățat zona accidentului, imagini groaznice ale carnajului erau încărcate pe forumuri de internet obscure din Rusia, frecventate de prietenii și clienții lui McColo. Printre primele care au difuzat știrea morții lui Kolea s-a aflat Crutop.nu, un forum rusesc de hackeri, care număra între cei 8 000 de membri ai săi pe unii dintre cei mai importanți spammeri din lume. Membrii Crutop.nu care au difuzat poze și informații despre eveniment erau unii dintre cei mai buni clienți ai lui McColo; mulți s-au simțit obligați (iar dacă n-au făcut-o, li s-a bătut obrazul în mod public de către administratorii forumurilor) să ajute cu bani familia lui Kolea pentru organizarea funeraliilor. Înmormântarea acestuia a fost un eveniment important în lumea subterană a criminalității informatice.

Câteva zile mai târziu, membrii comunității pestrițe a spammerilor din Moscova s-au adunat pentru a-i aduce un ultim omagiu. Ceremonia a avut loc în aceeași biserică în care Kolea fusese botezat cu aproape 23 de ani în urmă. Printre cei prezenți s-au numărat Igor „Desp" Gusev și Dmitri „SaintD" Stupin, administratori ai SpamIt și GlavMed, până de curând cei mai mari sponsori de spam* din lume și două personaje ce vor juca un rol-cheie în această carte.

La înmormântare a participat și hackerul Dmitri „Gugle" Necivolod, pe atunci în vârstă de 25 de ani, care avea o legătură strânsă cu botnetul Cutwail, un monstru care a infectat zeci de milioane de calculatoare din întreaga lume și

* Ar trebui amintit că Gusev a negat în mod public faptul că a difuzat spam și s-a ocupat de SpamIt, deși n-a făcut acest lucru în discuțiile pe care le-am avut cu el.

le-a folosit pentru a distribui spam. Necivolod câştigase deja milioane de dolari folosind botnetul pentru a trimite e-mailuri nesolicitate în beneficiul GlavMed şi SpamIt către milioane de persoane din întreaga lume. În prezent, Cutwail a rămas unul dintre cele mai mari şi mai active botneturi de spam – deşi acum este administrat cu siguranţă de mai multe persoane (despre acest lucru, a se vedea capitolul 7, „Să-i cunoaştem pe spammeri").

De ce trebuie să amintim de prezenţa acestor trei indivizi la un eveniment atât de important pentru criminalitatea informatică? Fiindcă activitatea lor (asemenea celei a lui Kolea şi a sute de alţi indivizi) ne afectează zi de zi într-un mod bizar, dar semnificativ: spamul.



Spamul a devenit impulsul principal al dezvoltării de malware – programe care ne atacă zilnic calculatoarele şi care vizează identitatea, siguranţa, banii, familiile şi prietenii noştri. Aceste botneturi sunt paraziţi virtuali care trebuie îngrijiţi şi hrăniţi în mod constant pentru a rămâne cu un pas înaintea antivirusilor şi a firmelor de securitate care încearcă să le distrugă. Pentru ca aceste colonii de PC-uri controlate să prospere, spammerii (sau botmasterii – termenii sunt sinonimi) trebuie să răspândească şi să modifice în permanenţă erorile digitale cu care se hrănesc. Deoarece antivirusii curăţă în mod regulat calculatoarele infectate, folosite pentru expedierea de spam, operatorii botneturilor trebuie să atace continuu, să capete controlul asupra unor computere noi şi să creeze alte modalităţi de infiltrare în cele infectate anterior.

Această cursă a înarmării tehnologice necesită dezvoltarea, producerea şi distribuirea de malware tot mai greu detectabil, care să poată scăpa de antivirusii şi instrumentele antispam care evoluează la rândul lor. Hackerii aflaţi în spatele acestor botneturi gigantice folosesc spamul şi ca o formă de autoapărare. Aceleaşi botneturi care difuzează spam învechit sunt

utilizate pentru a distribui e-mailuri nesolicitate care conţin versiuni noi de malware, ajutând la răspândirea infecţiei. Spammerii reinvestesc adesea câştigurile obţinute din spam în crearea de malware mai bun, mai puternic, mai bine disimulat, în stare să evite antiviruşii, programele antispam şi firewallurile. Ecosistemul spam este o maşinărie infracţională tehnico-socială în continuă evoluţie, care se autoalimentează.

Deocamdată, răufăcătorii care au dezlănţuit această molimă digitală reuşesc să fie net superiori industriei de securitate. Companiile antivirus informează că se străduiesc să clasifice şi să combată în *medie 82 000 de noi variante de malware care atacă zilnic computerele*, iar un procent important din aceste tulpini este menit să transforme computerele infectate în zombi de spam, care pot fi apoi controlaţi de la distanţă de atacator. Cei de la McAfee, marele producător de programe de securitate, au declarat că au detectat 14 milioane de malwareuri noi numai în primul trimestru al anului 2013.

Desigur însă că toate astea au un preţ şi pentru spammeri. În cazul lui Cutwail, întreţinerea reţelei presupune existenţa unor echipe de dezvoltatori de software şi de personal tehnic care lucrează 24 de ore pe zi, 7 zile pe săptămână. Asta se datorează faptului că programul care pune în mişcare botneturi de felul lui Cutwail este în mod obişnuit închiriat de alţi spammeri, care solicită frecvent modificări ale codului sau add-onuri capabile să ajute programele bot să funcţioneze corespunzător în infrastructura lor infracţională.

Abia trecut de 30 de ani, moscovitul Igor Vişnevski a fost unul dintre cei câţiva hackeri care au avut o colaborare strânsă cu Necivolod la Cutwail. (Vişnevski a pornit în cele din urmă pe cont propriu, creând o versiune rivală a lui Cutwail, pe care obişnuia de asemenea s-o utilizeze pentru spam şi s-o închirieze altor spammeri. A acceptat să fie pentru noi un fel de

Vergiliu* virtual şi să ne conducă prin această ciudată şi nefamiliară lume subterană a spammerilor, motiv pentru care este menţionat în toată cartea.) „Am avut un birou pentru Gugle [Necivolod, pronunţat asemenea cuvântului englezesc «Google»], cu programatori şi personal de asistenţă tehnică. Uneori treceam pe acolo, dar n-am lucrat de acolo", îşi amintea Vişnevski într-o conversaţie pe chat. Spunea că biroul lui Gugle avea minimum cinci programatori cu normă întreagă şi tot atâţia oameni care se ocupau cu asistenţa tehnică. Aceştia lucrau non-stop, în ture, inclusiv în weekend, pentru a răspunde cât mai bine cerinţelor clienţilor.

Firme de găzduire precum McColo au atras clienţi ca producătorii lui Cutwail deoarece au rămas on-line în ciuda presiunilor semnificative exercitate de autorităţile interne şi externe în vederea suprimării siteurilor dubioase sau ilicite pe care le găzduiau. Potrivit lui Vişnevski, serverele lui McColo erau bine cunoscute pentru viteza lor constantă şi pentru că erau „bulletproof" (blindate), adică imune la cererile de închidere depuse de alţi furnizori de servicii de internet (ISP) sau de autorităţi străine.

La scurt timp după moartea lui Kolea, McColo s-a grăbit să asigure comunitatea criminalităţii informatice că, deşi cel mai cunoscut membru al companiei murise, aceasta avea să-şi continue activitatea ca până atunci. Partenerul lui Kolea, Aleksei, a răspândit mesajul pe mai multe forumuri frecventate de infractorii informatici, încercând să-i asigure pe clienţii companiei că neplăcutul eveniment nu va duce la întreruperea serviciului.

Comunitatea criminalităţii informatice nu trebuia convinsă ca să rămână. Serviciul era găzduit mai ales în SUA şi era ieftin, fiabil şi rapid. În anul care a urmat morţii lui Nikolai, Necivolod

* Aluzie la faptul că, în celebrul poem al lui Dante, *Divina Comedie*, marele poet roman Vergiliu apare drept călăuză a autorului în infern şi purgatoriu (n. red.).

și majoritatea principalilor botmasteri de spam aveau să-și păstreze la McColo serverele folosite la controlul botneturilor.

Asta până în seara zilei de 11 noiembrie 2008, când un reportaj apărut în *Washington Post* despre concentrarea masivă de activități rău intenționate la furnizorul de servicii de găzduire i-a determinat pe cei doi furnizori ai conexiunii McColo la internet să decupleze simultan compania. Într-o clipă, volumul de spam a scăzut cu până la 75% în toată lumea, deoarece milioane de boți de spam au fost deconectați de la serverele lor și împrăștiați în cele patru colțuri ale lumii ca niște oi lipsite de păstor.

Închiderea lui McColo a lovit direct la buzunar botmasteri ca Necivolod și Vișnevski. Spammerii care închiriau botneturi au asaltat cu plângeri Crutop.nu și alte forumuri dedicate fraudelor, arătând că au pierdut sume substanțiale și vrând să știe ce măsuri se vor lua.

„În cazul McColo, aveam servere din SUA care posedau o viteză bună, își amintea Vișnevski. Când McColo a fost închisă, a trebuit să închiriem servere mult mai lente din China și alte țări care sunt praf" în ceea ce privește capacitatea de a face față unor plângeri privind abuzurile.

Dornici să demonstreze că puțini credeau că McColo va dispărea vreodată – chiar și după moartea lui Kolea – mulți spammeri au păstrat direct pe serverele companiei o altă componentă majoră și costisitoare a operațiunilor lor: liste imense cu adrese de e-mail.

„Toți și-au pierdut listele acolo", a spus Vișnevski, subliniind că, după închiderea lui McColo, el și Necivolod au pierdut o listă foarte mare și valoroasă, cu peste două miliarde de adrese de e-mail.

Moartea lui Kolea și desființarea lui McColo au fost momente hotărâtoare, deoarece au însemnat începutul sfârșitului unei ere în care spammerilor și baronilor crimei informatice li

se îngăduise să opereze într-o siguranță relativă. Pe vremea aceea, peste 90% din totalul e-mailurilor trimise în întreaga lume erau nesolicitate, iar majoritatea făceau reclamă unor presupuse siteuri farmaceutice. În următorii patru ani, închiderea altor ISP-uri ilicite, furnizori de găzduire web și mari botneturi de spam avea să reducă masiv volumul de e-mail nesolicitat și să coincidă cu arestarea sau condamnarea la închisoare a câtorva spammeri de marcă.

Desființarea companiei McColo a reprezentat de asemenea începutul unei noi ere a spamului, prin declanșarea unui îndelungat și costisitor conflict pentru supremație pe care îl vom analiza în această carte. „Războiul farma", așa cum i-au spus cei din lumea criminalității informatice și a securității informatice, a irupt sub forma unei încleștări sălbatice între doi dintre cei mai mari sponsori ai spamului farmaceutic – care a prins la mijloc utilizatori ca mine și ca dumneavoastră, care nu au bănuit nimic.



De o parte s-au aflat Dmitri Stupin și Igor Gusev, menționați mai înainte, și operațiunile lor farmaceutice, GlavMed și SpamIt. De cealaltă parte s-a aflat Rx-Promotion, o afacere farmaceutică ilicită de pe internet, inițiată de fostul partener de afaceri al lui Gusev, moscovitul de 35 de ani Pavel Vrublevski. În mod oficial, Vrublevski era directorul executiv al companiei ChronoPay, una dintre cele mai mari firme rusești de procesare a plăților on-line, pe care acesta a fondat-o împreună cu Igor Gusev.

În secret, Vrublevski avusese legături strânse cu lumea subterană a criminalității informatice, ajutând tot soiul de tâlhari on-line să obțină procesarea cardurilor de credit pentru afacerile lor dubioase și încasând o parte însemnată din câștig. Tot Vrublevski este cofondatorul și administratorul popularului forum pentru spammeri Crutop.nu și o altă figură centrală a războaielor informatice care ne-au transformat în prezent într-o națiune a spamului – ba chiar într-o lume a spamului.

În 2010, cercetam deja de peste un an și scriam despre acuzațiile de corupție aduse lui Vrublevski, ca și despre presupusele sale legături cu spammerii care lucrau pentru programulfarmaceuticilicitRx-Promotion,maiîntâicareporter de investigații pentru *Washington Post* și apoi pentru propriul meu site de informații despre securitatea informatică, KrebsOnSecurity.com. Pe măsură ce am avansat însă, am vrut să aflu mai multe despre e-mailurile nesolicitate și despre problema securității informatice: cine o provoca și cum putea fi rezolvată. Era clar că și alții gândeau ca mine.

Înainte de războiul de uzură dintre baronii spamului pe care îl vom analiza în această carte, au existat surprinzător de puține informații publice sigure pentru a putea răspunde la întrebările esențiale referitoare la problema spamului, cum ar fi:

- Cine cumpără produsele promovate în e-mailurile nesolicitate, cum ar fi Viagra, medicamente care se eliberează pe bază de rețetă, chiar și poșete Gucci? Ce îi determină pe oameni să cumpere și să înghită niște pastile cărora le fac reclamă vânzători agresivi și necunoscuți?
- Sunt aceste medicamente reale sau sunt falsuri ineficiente și, posibil, mortale?
- Cine profită de pe urma distribuirii spamului? Cum sunt împărțite profiturile și unde merg banii?
- De ce industria farmaceutică – una dintre cele mai bogate și mai influente din lume – este aparent neputincioasă în ceea ce privește oprirea hoției și a însușirii ilegale a produselor, mărcilor și clienților săi?
- De fapt, de ce este atât de ușor să plătești cu un card de credit aceste medicamente contrafăcute cărora li se face masiv reclamă prin spam?
- Conturile clienților care folosesc cardul de credit sunt sparte sau revândute după ce au cumpărat de la spammeri?

Ce se întâmplă dacă nici măcar n-au cumpărat? Sunt totuşi în pericol?

• Ce pot face consumatorii, factorii de decizie şi autorităţile în aşa fel încât să ţină sub control epidemia de criminalitate informatică?

Acestea sunt câteva dintre întrebările pe care le-au pus oamenii când le-am spus că scriu o carte despre spam. La început, le-am putut oferi drept răspuns doar ipotezele mele. Chiar şi când am cerut sfatul unor presupuşi experţi în spam, am descoperit că nici cele mai importante autorităţi mondiale în domeniu nu aveau un răspuns ferm. Mulţi mi-au dat răspunsuri standard, care păreau să se bazeze pe câteva studii de caz foarte cunoscute, dintre care unele fuseseră finanţate de mari companii farmaceutice sau de securitate.





Bazele de date folosite la spamul farmaceutic pe care am reuşit să le obţin de la Rx-Promotion şi GlavMed–SpamIt în timpul războiului farma a schimbat situaţia, oferind o imagine despre aproape toate aspectele semnificative ale activităţii celor mai mari organizaţii de spam din lume. Poate ca o ironie a sorţii, spammerii înşişi mi-au oferit această posibilitate de a arunca o privire asupra acţiunilor lor necurate ce ne afectează viaţa de zi cu zi.

Hackeri loiali lui Gusev şi Vrublevski au făcut ca aceste informaţii să ajungă la autorităţi şi la mine în tentativa de a se sabota reciproc. Bazele lor de date au oferit o imagine fără precedent a operaţiunilor şi profiturilor zilnice ale misterioaselor carteluri internaţionale ale medicamentelor, din care fac parte spammeri, creatori de viruşi, furnizori dubioşi şi expeditori. Informaţiile respective au stat la baza multor aspecte semnalate de mine în cartea de faţă.

Mai important – şi mai alarmant – este faptul că această arhivă conţinea şi informaţii demografice, medicale şi financiare

despre milioane de clienți – în majoritate consumatori din SUA – care cumpăraseră medicamente pe bază de rețetă de pe rețelele de spam după ce primiseră o solicitare prin e-mail sau după ce căutaseră on-line asemenea medicamente.

Bazele de date au oferit o imagine reală a cererii ascunse, dar înfloritoare de medicamente ieftine eliberate pe bază de rețetă, ce pare în mare măsură impulsionată de americani interesați de medicamente mai ieftine, care pot fi procurate în mod discret.

Având în vedere amenințarea tot mai mare reprezentată de e-mailurile nesolicitate și atacurile la adresa securității informatice care îi afectează în mod direct pe consumatori și companii (a se vedea relatarea difuzată de mine în mass-media în decembrie 2013 despre spargerea bazei de date ale posesorilor cardurilor de credit Target – un atac informatic care a compromis informațiile financiare a milioane de americani și i-a obligat pe și mai mulți să solicite noi carduri de credit), ne-am putea întreba de ce guvernele, autoritățile și corporațiile nu iau o poziție mai fermă pentru oprirea valului de spam și criminalitate informatică ce ne afectează pe toți.

Una dintre cauzele reacției slabe a comunității internetului față de epidemia de malware și spam este aceea că mulți factori de decizie și experți în criminalitatea informatică tind să ignore spamul, considerându-l o problemă neplăcută ce poate fi rezolvată sau cel puțin atenuată printr-o combinație adecvată de tehnologie și măsuri legale. Pentru mulți dintre noi, spamul devenise aproape sinonim cu poanta unui banc, din cauza asocierii cu pilulele pentru mărirea penisului și cu medicamentele pentru disfuncția erectilă ca Viagra și Cialis. Credeam că nu suntem afectați dacă nu deschidem e-mailurile sau nu cumpărăm nimic din ceea ce promovau acestea.

Din păcate, această atitudine scoate în evidență o greșeală des întâlnită, dar fundamentală privind amenințarea pe care

spamul o reprezintă pentru toți: puterea distructivă a botneturilor și a programatorilor nechibzuiți care le asigură funcționarea. Botneturile create și gestionate de membrii SpamIt, Rx-Promotion și ai altor programe de afiliere pe bază de spam n-au fost utilizate exclusiv pentru distribuirea de spam. Răufăcătorii de pe internet asigură în mod curent, contra cost, accesul la asemenea mașinării infracționale pentru a le masca locația reală on-line, deoarece botneturile le permit să-și amplifice traficul pe internet printr-o multitudine de PC-uri infectate, care sunt în mare măsură nedetectabile.

Escrocii care apelează la aceste botneturi le folosesc în mod regulat și pentru a strânge nume de utilizator și parole de la PC-urile gazdă, furând totul, de la date de identificare bancară on-line la chei digitale care pot oferi acces la prețioasele secrete ale unor companii mari și mici. Răufăcătorii aflați la cârma unora dintre cele mai active botneturi din lume controlează deja mii de computere zombi ale unor companii importante, care permit atacatorilor să expedieze spam către persoanele care folosesc serverele mai puternice ale acestor corporații și să extragă datele confidențiale din sistemele lor interne.

Botneturile sunt și cauză altor amenințări grave. În mod frecvent, ele sunt închiriate pentru a fi utilizate în operații foarte riscante de extorcare desfășurate pe internet, cunoscute drept atacuri „DDoS" (*distributed denial of service*). În astfel de cazuri, escrocii solicită companiilor zeci de mii de dolari ca taxă de protecție. Dacă acestea refuză să plătească, botmasterii ordonă armatelor lor de PC-uri infectate să asedieze siteul companiei vizate cu atât de mult trafic nesolicitat, încât să nu mai poată primi vizitatori legitimi. Compania extorcată fie plătește, fie rămâne off-line până când atacatorii renunță (sau, dacă își permite, angajează o firmă autorizată anti-DDoS care s-o ajute să respingă aceste atacuri).

Atacurile DDoS motivate politic sau ideologic pot să deconecteze de la internet țări întregi și să reducă la tăcere critici

sau protestatari. În 2008, un puternic atac DDoS motivat politic, lansat împotriva Estoniei, țară care a făcut parte din URSS și care dispune de o vastă rețea de conexiuni la internet, a scos din uz majoritatea siteurilor guvernamentale vreme de câteva zile, a întrerupt operațiile bancare electronice timp de câteva ore, a făcut să cadă cea mai mare rețea de telefonie mobilă din țară și a perturbat funcționarea rețelei naționale pe care estonienii se bazează în caz de urgență medicală.

Un atac de o asemenea intensitate a atras atenția și îngrijorarea guvernului și armatei SUA. Atacurile informatice fuseseră identificate ca o amenințare gravă, reală la adresa mașinăriei de război americane. Într-un important discurs rostit în luna mai a anului 2009 la Casa Albă, președintele Obama a declarat că amenințarea informatică este una dintre cele mai serioase probleme economice și de securitate națională cu care se confruntă actualmente America.

În ciuda îngrijorării guvernelor, reacția factorilor de decizie la nivel înalt față de mecanismele organizaționale și tehnologice care alimentează epidemia de spam a fost apatică în cel mai fericit caz, iar pe alocuri, practic inexistentă. Deși avem de a face cu o amenințare capabilă să perturbe funcționarea infrastructurii unor țări întregi, să blocheze rețele de comunicații vitale, să intoxice populația prin răspândirea de bunuri de consum contrafăcute și să stimuleze dezvoltarea unei economii ilegale, guvernele din întreaga lume n-au făcut mare lucru pentru a-și proteja cetățenii de aceste armate informatice invadatoare.

Mulți legiuitori din SUA și din alte părți ale lumii se folosesc de epidemia de criminalitate informatică pentru a face lobby în vederea modificării legilor privind felul în care poliția și autoritățile statului pot culege date despre cetățeni. Sancțiunile mai aspre împotriva criminalității informatice nu i-au descurajat însă nici pe atacatori și nici activitățile

spammerilor dornici să se îmbogăţească şi ale hoţilor moderni, care operează pe internet. Majoritatea legilor americane privind securitatea internetului propuse şi aprobate în ultima vreme s-au concentrat asupra unor vagi iniţiative de îmbunătăţire a securităţii infrastructurii informaţionale esenţiale a ţării: computerele şi sistemele interconectate care administrează totul, de la fabrici şi instalaţii de tratare a apei până la reţeaua electrică.

Eforturile legislative făcute în ultima perioadă în SUA cu privire la combaterea criminalităţii informatice s-au lovit însă de opoziţia fermă a partizanilor principiului confidenţialităţii şi a publicului larg. Când a încercat să adopte o lege care i-ar fi obligat pe furnizorii de servicii de internet să blocheze accesul publicului la siteuri care comercializează produse contrafăcute, Congresul SUA s-a confruntat aproape cu o revoltă a contribuabililor. Rezistenţa s-a manifestat de cele mai multe ori sub forma unor demonstraţii on-line abil planificate.



Între timp, câteva arestări ale unor personaje-cheie şi acţiuni desfăşurate împotriva botneturilor de spam şi a principalilor actori din lumea subterană a criminalităţii informatice par să fi făcut, pentru destabilizarea acestei industrii, mai mult decât orice propunere legislativă avansată până acum. Aşa cum o ilustrează numeroasele exemple din această carte, este posibil ca guvernele să producă un impact maxim asupra criminalităţii informatice nu adoptând legi noi sau mărind sancţiunile corespunzătoare diverselor delicte informatice, ci aplicând mai eficient legile existente, exercitând presiuni asupra corporaţiilor din întreaga lume în vederea abordării acestei probleme într-un mod adecvat propriilor interese şi extinzând domeniul de acţiune al autorităţilor naţionale.

Asta nu înseamnă că răspunsul la problema combaterii spamului şi a botneturilor îl au exclusiv guvernele. Dimpotrivă, aşa cum vom vedea în cartea de faţă, unele dintre măsurile cele mai eficiente luate împotriva acestui flagel

s-au datorat eforturilor corporațiilor de a-și proteja interesele financiare, clienții, mărcile comerciale și imaginea publică – și chiar eforturilor consumatorilor înșiși.

În ultimă instanță, spamul și toate problemele asociate lui se vor diminua foarte puțin fără un impuls concertat din partea unora dintre cele mai bogate și mai puternice comunități din lume, inclusiv a industriei farmaceutice, a firmelor care gestionează plățile cu carduri de credit și a sectorului bancar, a legiuitorilor și autorităților din toată lumea, ca și din partea unor oameni ca noi, care suntem în majoritate ținte și victime inocente ale spammerilor și hackerilor. Este timpul să facem ceva în legătură cu această epidemie globală, pentru a ne proteja identitatea, conturile bancare, familiile și viața înainte de a fi prea târziu.

# Capitolul 2

# BULLETPROOF

Pentru a înțelege amenințarea pe care o reprezintă spamul pentru noi toți, este esențial să examinăm mai întâi cotloanele întunecate ale lumii criminalității informatice și să înțelegem ce se ascunde acolo: răpiri, mituiri, extorcări, șantaje, corupție. Toate acestea s-au numărat printre metodele de afaceri utilizate în mod obișnuit de cei care au creat primele paradisuri de criminalitate informatică: bârlogurile virtuale ale piraților de pe internet.

Aceste companii de găzduire web – cele mai multe dintre ele cu sediul în Rusia și fostele state sovietice – erau frecvent denumite „rețele bulletproof" sau „furnizori de găzduire bulletproof", deoarece obținuseră suficientă protecție politică și operațională, printr-o multitudine de metode (legale sau ilegale), pentru a le face practic imune în fața legii. Ba chiar aveau o influență atât de mare, încât au reușit să rămână on-line în ciuda presiunilor exercitate de guverne și autorități străine pentru a fi deconectate de la rețea împreună cu clienții lor, care traficau în mod invariabil pe web bunuri și servicii dubioase sau ilicite.

Una dintre fruntașe, McColo Corp., era maestră în acest sens. Bineînțeles că nu Nikolai, tânărul întreprinzător despre a cărui moarte violentă în urma unui accident rutier am vorbit la începutul capitolului 1, a inventat afacerea atragerii și găzduirii on-line de întreprinderi bazate pe criminalitatea informatică.

Mai degrabă, asemenea inovatorilor din alte domenii, el s-a ridicat pe umerii giganților din domeniul criminalității informatice dinaintea sa, perfecționând, prin faptul de a se fi concentrat pe eficiență, un vechi model de afaceri: i-a eliminat pe intermediari, a redus masiv prețurile și a investit în rețele mai fiabile și mai rapide.

Mai mult decât atât, McColo s-a distins prin aceea că a dobândit reputația de furnizor de servicii de găzduire bulletproof, care oferea asistență tehnică și pentru clienți de cea mai bună calitate. Acestea erau aspecte pe care pionierii în domeniu le trecuseră cu vederea, probabil din cauza concurenței foarte reduse.

Pentru a înțelege însă cum a ajuns McColo să domine lumea subterană a criminalității informatice, va trebui să știm cum și de ce au eșuat predecesorii săi. Furnizorii de găzduire bulletproof care au pregătit terenul pentru afacerea tânărului Nikolai au, de asemenea, o legătură strânsă cu începutul carierei celor doi baroni ai criminalității informatice a căror îndelungată rivalitate constituie subiectul principal al acestei cărți. Mai înainte de orice, o rețea a înlesnit ascensiunea lui McColo, declanșarea războiului farma și folosirea multora dintre practicile dubioase sau ilegale care ne amenință în prezent securitatea on-line.

La mijlocul anului 2007, Russian Business Network (RBN) – un obscur conglomerat de furnizori de găzduire web, cu sediul în Sankt Petersburg – își consolidase printre experții în securitate reputația de centru al criminalității informatice. În repetate rânduri, când anchetatorii au pornit pe urma banilor și dovezilor furnizate de siteuri care vindeau pornografie infantilă sau software piratat, au ajuns la siteuri aflate în proprietatea RBN. Când au încercat să închidă siteuri care răspândeau viruși și escrocherii de tip „phishing", folosind e-mailuri în care se dădeau drept bănci și încercau să-i convingă pe utilizatori să introducă parolele propriilor conturi pe siteuri

bancare false, au constatat că, în majoritatea cazurilor, acestea erau clienți ai RBN.

RBN era întruchiparea perfectă a primilor furnizori de găzduire bulletproof, adevărate refugii în care clienții puteau expune și oferi practic orice fel de conținut on-line – indiferent cât de ilegal sau ofensator – atâta vreme cât continuau să plătească taxe exorbitante, care puteau crește fără preavizare. Un server web de bază la RBN costa între 600 și 800 de dolari pe lună, adică de peste zece ori mai mult decât percepeau în acel moment de la clienții obișnuiți majoritatea furnizorilor de servicii de găzduire autorizați.

Aceste taxe nu umpleau pur și simplu buzunarele furnizorilor respectivi, ci erau esențiale pentru supraviețuirea lor. De exemplu, o parte a veniturilor respective se scurgea de la șefii RBN la autoritățile locale și la politicienii corupți din regiune, unii dintre ei fiind dispuși să se uite în altă parte atunci când soseau reprezentanții unor autorități străine dornici să se intereseze de niște siteuri care promovau activități ilegale găzduite pe rețelele RBN.

David Bizeul, specialist francez în securitatea informatică, care a efectuat o analiză complexă a RBN în perioada sa de glorie de la jumătatea anului 2007, a afirmat că rețeaua avea o echipă specială, responsabilă cu rezolvarea reclamațiilor de abuzuri, dar că ea avea doar menirea de a face ca RBN să pară un furnizor de servicii de internet (ISP) legitim.

„RBN are o echipă de cercetare a abuzurilor – folosită pentru a-i conferi o imagine respectabilă – care vă va cere un act de acuzare rusesc pentru a cerceta" o reclamație de abuz sau de tratament umilitor, scria Bizeul în 2007. „Desigur, acest act de acuzare este foarte greu de obținut. Nu este atunci un paradis pentru șarlatani?"

Originile exacte ale Russian Business Network sunt învăluite în mister. Poate din acest motiv, mulți experți în securitatea computerelor au atribuit majoritatea activităților rău

intenționate de pe internet celor aflați în spatele RBN, indiferent dacă activitățile respective aveau sau nu aveau legături evidente cu infama rețea de găzduire.

Dacă RBN devenise un fel de sperietoare digitală pentru mulți, această reputație fusese câștigată totuși cu greu. Potrivit reportajelor apărute în presă și unor surse apropiate companiei, RBN s-a născut din nevoia răufăcătorilor informatici de a dispune de o găzduire web mai stabilă și mai sigură pentru unele dintre afacerile lor ilegale – în special pornografia extremă și pornografia infantilă. De fapt, rădăcinile RBN se întind până în industria pornografiei infantile și până la grupările de crimă organizată din Minsk (Belarus).

La începutul noului mileniu, Aleksandr Rubațki, un tânăr belarus inteligent, în vârstă de 22 de ani, era pregătit să calce pe urmele tatălui său, un respectat locotenent-colonel de miliție. Rubațki era însă mult mai interesat și priceput la computere, motiv pentru care, în cele din urmă, a renunțat la academia de miliție.

Victor Ceamkovski, cineast și jurnalist de investigație din Belarus, care a studiat începutul carierei lui Rubațki, a declarat că talentul acestuia a atras atenția grupărilor locale de crimă organizată, care considerau că se puteau obține câștiguri importante din procesarea plăților pe internet, mai ales pentru afacerile din domeniul pornografiei. Potrivit lui Ceamkovski, Rubațki s-a asociat în 1995 cu Ghennadi Loghinov, un tânăr huligan, al cărui frate era șeful grupării militante de crimă organizată intitulate „Satul" din Minsk. Treaba lui Rubațki nu era le forțeze mâna oamenilor, ci să găsească pur și simplu baze de date pentru a fura conturi de carduri de credit care puteau fi golite sau vândute pe bani gheață.

În primăvara anului 2001, Rubațki a început să-și caute un loc de muncă adevărat și a fost angajat ca specialist în computere la CyberPlat, în acel moment, cea mai mare firmă de procesare a plăților on-line din Rusia. În calitatea pe care

o avea, i s-au dat fonduri și autoritatea de a angaja peste 12 programatori. Misiunea lui era să formeze o echipă care să poată crea următoarea generație de platformă de plăți a CyberPlat.

Ziarul belarus *BelGazeta* a făcut cunoscut faptul că CyberPlat l-a plătit pe Rubațki și să testeze cu rigurozitate computerele firmei în căutarea unor vulnerabilități de securitate care o puteau expune la riscul de a pierde informații. Ulterior, compania avea să susțină că angajatul a abuzat de acest lucru, descărcând o copie a bazei de date despre clienți. Rubațki le-a declarat procurorilor că și-a însușit datele respective doar pentru a putea demonstra breșele de securitate găsite de echipa lui. Angajatorul său nu i-a acceptat însă explicația. Miliția a efectuat o descindere în casa în care lucrau Rubațki și hackerii lui, ridicând suficiente dovezi pentru ca acesta să poată fi acuzat de furt. Într-un final, justiția din Belarus a dat dreptate firmei CyberPlat și l-a condamnat pe Rubațki la șase luni de închisoare. (Sentința a fost ulterior suspendată.)

Rubațki avea să se răzbune însă. Înainte de terminarea procesului, lista clienților firmei CyberPlat a ajuns în posesia autorităților. Anchetatori din SUA și alte țări suspectaseră de mult că majoritatea plăților către siteurile care vindeau pornografie infantilă se făceau prin intermediul unor conturi comerciale asociate cu CyberPlat și partenerul său moscovit, Bank Platina, iar acum aveau o dovadă indubitabilă.

La mijlocul anului 2002, CyberPlat a fost prinsă într-un scandal internațional când cotidianul rusesc *Kommersant* a anunțat că printre clienții lui CyberPlat se numărau zeci de siteuri care ofereau contra cost acces la imagini și videoclipuri cu pornografie infantilă. În urma scandalului, CyberPlat a concediat 40% din personal, inclusiv membri ai conducerii.

Între timp, Rubațki a fost lăsat să lucreze mai departe pe piața foarte profitabilă a procesării plăților pentru siteurile

obscure care ofereau pornografie infantilă. În același timp, Loghinov era hotărât să întărească securitatea operațională și fizică a afacerii sale. Miliția nu va mai putea face niciodată atât de ușor o descindere la căsuța hackerilor.*

Anticipând activitatea de pionier în afacerile bulletproof din domeniul găzduirii web, Rubațki a încercat să-și asigure protecția locală și fizică a autorităților pentru a putea să-și desfășoare mai departe activitatea fără întrerupere sau amestec din partea nimănui. Dacă miliția hotăra să mai facă o descindere, cel puțin Rubațki știa că urma să aibă loc și avea posiblitatea să ascundă sau să distrugă dovezi incriminatoare.

Potrivit documentarului *Operation Consortium* realizat de Ceamkovski, ca și altor surse rusești, Loghinov și asociații lui au înțesat casa cu dispozitive de securitate, inclusiv camere de luate vederi cu circuit închis și sisteme de alarmă. Echipa lui Loghinov a achiziționat de asemenea arme de foc, stații de radio folosite de miliție și uniforme. Au beneficiat chiar de instrucție militară din partea unui fost ofițer al KGB – poliția secretă și serviciul de informații al Uniunii Sovietice.

Se pare că banda lui Loghinov a urmat un curs intensiv destinat agenților de teren ai KGB, care a inclus teste fizice și psihologice de rezistență, precum și o instruire specializată în abilități medicale și tehnice. „Inițial, au trebuit chiar să susțină examene [scrise]", a declarat, în documentarul lui Ceamkovski, Igor Parmon, adjunct în Ministerul Afacerilor Interne din Belarus. „Erau chiar pedepsiți dacă lipseau de la cursuri."

Într-un articol publicat în 2004 în *Belarusian Business News* se descrie cum a reacționat grupul lui Loghinov când a aflat că omul de afaceri Evgheni „Pet" Petrovski își crea propria afacere de procesare a cardurilor de credit care urma să

* Deși nu am putut da de urma lui Rubațki, potrivit agenției belaruse Telegraph (agenția națională de știri), el este în prezent dat în urmărire prin Interpol.

deservească industria pornografiei infantile, o companie numită Sunbill (redenumită ulterior BillCards). Grupul respectiv a hotărât să aplice cunoştinţele de luptă recent dobândite pentru a elimina – sau cel puţin pentru a intimida – concurenţa. Presupusul rol jucat de Petrovski în apariţia primei afaceri de procesare a cardurilor pentru siteurile de pornografie infantilă a fost, de asemenea, atestat în 2004 de Computer Crime Research Center, o organizaţie nonprofit cu sediul la Odessa (Ucraina), care culege date despre criminalitatea informatică transnaţională.

Pe când se afla la volanul maşinii sale, Petrovski a fost oprit de un bărbat care s-a dat drept miliţian, iar când a coborât din automobil, aşa cum i se ceruse, a fost răpit de nişte bărbaţi mascaţi. După ce au ajuns la casa lor de la periferia Minskului, răpitorii i-au contactat pe asociaţii lui Petrovski şi au cerut un milion de dolari pentru eliberarea sa. Nu au primit însă niciun ban. Când autorităţile locale au început să se apropie de locul în care se aflau aceştia, răpitorii au fugit cu Petrovski la Moscova. În noiembrie 2012, autorităţile ruse şi belaruse au găsit ascunzătoarea bandei lui Loghinov şi i-au arestat pe răpitori. Petrovski a fost găsit viu şi relativ nevătămat.*

Potrivit lui Ceamkovski, Rubaţki era foarte concentrat pe hacking şi furt de date financiare din magazinele on-line şi n-a ştiut de activităţile paramilitare ale tovarăşilor săi. Când a aflat că grupul lui Loghinov a fost arestat pentru răpire şi extorcare, Rubaţki a fugit din Belarus în Rusia, la Sankt Petersburg.

Dintr-un birou închiriat în centrul oraşului, se pare că el a colaborat cu angajaţi ai Alfa Bank de la Moscova pentru a înfiinţa un sistem de plăţi complet nou, numit „Alfa-Pay". Sistemul era destinat să proceseze plăţi pentru pornografia infantilă şi să protejeze afacerea de perturbări sau ochi curioşi.

* Loghinov şi câţiva asociaţi au fost ulterior urmăriţi penal şi găsiţi vinovaţi de răpire şi alte delicte. Potrivit unui articol din *Ecommerce Journal*, se crede că Petrovski se ascunde în Ucraina.

Într-un reportaj publicat în 2006 în ziarul belarus *Evening Minsk*, se arăta că aceasta se baza pe o rețea de holdinguri care serveau ca intermediari pentru angajați din Belarus ce se ocupau de toate, de la fotografierea modelelor adolescente și preadolescente până la distribuirea conținutului și plata comisioanelor către revânzătorii materialelor fotografice.

„Cu ajutorul lui Rubațki", scria Ceamkovski, „a fost creat un holding uriaș, care realiza totul, de la ședințele foto și distribuirea pornografiei până la activitățile administrative, inclusiv plățile regulate, facturarea și plata comisioanelor. Experiența lui Rubațki cu privire la [...] siteurile dedicate pornografiei infantile a fost folosită în crearea unui sistem standardizat care putea fi ușor multiplicat."

Toate acestea pot părea o problemă limitată la Rusia și Europa de Est, unde este permisă existența unor companii dubioase, specializate în criminalitate informatică. Adevărul este însă că marea majoritate a clienților afacerii pomenite mai înainte erau americani dispuși să plătească peste 40 de dolari pe lună pentru un abonament la siteuri de pornografie infantilă, numite în lumea subterană siteuri „căpșunica" sau „lolita" (ultima fiind o referire la romanul cu același titlu al scriitorului rus Vladimir Nabokov). Potrivit unor reportaje apărute în presă, rețeaua lui Rubațki de siteuri de pornografie infantilă atrăgea zilnic peste 100 000 de vizitatori și genera venituri lunare de aproape 5 milioane de dolari.

În scurt timp însă, Alfa-Pay s-a trezit din nou concurată de firma de procesare a plăților BillCards a lui Petrovski. În acel moment, el era aliat cu Igor „Desp" Gusev, despre care se zvonea că fusese administratorul forumului secret Darkmasters.com, destinat webmasterilor (proprietarilor de siteuri) implicați în vânzarea de pornografie extremă, care includea pornografia infantilă.*

* Într-un interviu luat prin e-mail, Igor Gusev a recunoscut că cineva care folosea pseudonimul lui, „Desp", apărea ca administrator

Nu după multă vreme, Alfa-Pay a lui Rubaţki şi Bill-Cards a lui Petrovski încercau să se distrugă reciproc, potrivit afirmaţiilor lui Pavel Vrublevski, cofondator şi proprietar al companiei ruseşti ChronoPay, menţionată în capitolul 1, care a început, în 2003, să proceseze plăţi pentru webmasterii de siteuri pornografice. (În 2003, Gusev avea să i se alăture lui Vrublevski în calitate de cofondator al lui ChronoPay, care, ulterior, avea să eclipseze CyberPlat şi să devină cel mai mare serviciu de procesare a plăţilor on-line din Rusia.)

„Alfa-Pay a început o luptă acerbă cu BillCards, fiecare lansând atacuri informatice asupra celeilalte, încercând să se pună sub urmărire penală una pe cealaltă, trimiţând mass-mediei informaţii incriminatoare şi tot felul de alte mizerii", îşi amintea Vrublevski într-o discuţie din 2010, care avea să prefigureze în mod straniu disputa pentru supremaţie dintre el şi Gusev pentru piaţa on-line de produse farmaceutice contrafăcute. „Drept consecinţă, ambele companii s-au destrămat şi a urmat un scandal de proporţii."

Rubaţki a decis atunci că era timpul să abordeze un alt domeniu profitabil, dar mai puţin periculos: găzduirea web. Potrivit lui Vrublevski, belarusul a avut o întâlnire cu administratorii Eltel, un ISP local ale cărui reţele asigurau conexiunea la internet a unei mari părţi a oraşului Sankt Petersburg.

Vrublevski susţine că şefii Eltel au cumpărat pentru afacerea sa protecţia politică a Serviciului Federal de Securitate al Rusiei (FSB), succesorul KGB. Genul respectiv de acoperire, cunoscut sub numele de *kruşa*, „acoperiş" în limba rusă, era considerat necesar pentru orice afacere capabilă să

pe pagina de pornire a Darkmasters.com, dar a negat că el însuşi a fost vreodată administrator al forumului respectiv. În schimb, a declarat că a acceptat doar ca pe site să apară aprobarea sa în schimbul unei sume primite de la administratorul real – un alt webmaster pornografic care utiliza pseudonimul „Master". Pe de altă parte, Vrublevski subliniază că aceasta este „dovada" că Gusev a avut o legătură strânsă cu Russian Business Network.

genereze profituri sănătoase, întrucât acest lucru expunea afacerea la intervenții ale organelor penale și guvernamentale și chiar la acte de violență.

Potrivit lui Vadim Volkov, autorul cărții intitulate *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*, agenții FSB sunt adesea introduși ca angajați în companii rusești, pentru a le ajuta, chipurile, să lupte împotriva celor care ar putea încerca să le fure profiturile.

Volkov scrie că legislația rusă permite agenților FSB activi să fie „detașați la diverse întreprinderi și organizații, cu consimțământul directorilor lor. [...] Această prevedere a permis ca mii de ofițeri de securitate activi să dețină funcții în companii și bănci private în calitate de «consilieri juridici», cum era numită cu modestie funcția lor. Folosind legăturile pe care le aveau cu organizațiile de stat și sursele de informații ale FSB, ei îndeplineau rolul de «acoperiș», cum avea să fie numit ulterior – protejând firmele de extorcări și înșelăciunile grupărilor criminale și facilitând relațiile cu birocrația. Potrivit estimărilor făcute de experți, până la 20% dintre ofițerii FSB sunt implicați în afaceri neoficiale de tip «acoperiș»".

„Se știa că cei de la Eltel erau realmente nebuni și găzduiau pornografie infantilă și alte obscenități de acest fel fiindcă aveau o relație bună cu poliția locală, spunea Vrublevski într-o convorbire telefonică. Dar ISP-urile din amonte de Eltel le treceau în mod constant siteurile pe lista neagră, așa că Rubațki a venit cu ideea de a avea o legătură directă cu mari furnizori de servicii de internet precum Telia și Tiscali.* Având legătură directă, furnizorii de servicii de găzduire bulletproof nu mai stăteau la mila unor ISP-uri intermediare mai mici, care

* În prezent parte a companiei TeliaSonera, Telia a fost principala companie suedeză de telecomunicații cu filiale în Europa și Asia. Tiscali este o companie italiană de telecomunicații care oferă servicii pe plan intern, dar, la un moment dat, a furnizat servicii în toată Europa și Hong Kong.

puteau fi constrânse să decupleze RBN la cel mai mic semn de interes din partea autorităţilor.

Pentru a eluda acest obstacol, „Rubaţki a ajuns să cheltuiască o grămadă de bani pentru ca [Eltel] să aibă propriul canal de internet din străinătate", îşi amintea Vrublevski. „Şi l-au numit «Russian Business Network», prescurtat RBN."

Potrivit lui Vrublevski, Rubaţki l-a numit şef al proiectului RBN pe inteligentul tehnician Eugen I. Sergheienko, un hacker în vârstă de 25 de ani cunoscut în lumea subterană sub pseudonimul „Flyman".

În scurt timp, Flyman avea să devină sinonim atât cu RBN, cât şi cu epidemia globală de spam, RBN devenind un centru global al activităţilor informatice rău intenţionate, de la planurile de phishing până la mesajele privind impotenţa masculină care ne bombardează zilnic pe toţi.

În 2007, RBN era o forţă în domeniul criminalităţii informatice, devenind un adevărat magnet pentru tot felul de activităţi infracţionale on-line. Cercetătorii din mediul academic şi de la firmele private de securitate pe internet atrăgeau de peste un an atenţia cu privire la RBN, publicând nenumărate rapoarte despre numărul imens de escrocherii prin phishing, spam pentru mărirea penisului şi siteuri care găzduiau malware provenit de la ISP-uri cu probleme, ce contamina milioane de PC-uri conectate la internet din toată lumea. Majoritatea acelor rapoarte erau însă analize destul de tehnice, referitoare la câteva aspecte ale efectelor malefice produse de RBN: o nouă inovaţie malware, un centru de comandă botnet sau alte siteuri rău intenţionate apărute în „ograda" RBN.

Mi-am dat seama că nimeni nu centralizase toate cercetările disparate despre RBN şi nici nu încercase să le adune într-un raport care să dezvăluie activităţile rău intenţionate ale reţelei. La vremea respectivă, acele rapoarte au contribuit

treptat la slăbirea infrastructurii care menținea în funcțiune rețeaua RBN, așa încât mi s-a părut că demascarea ei într-o publicație de largă circulație putea să pună capăt pentru totdeauna afacerii în cauză.

Mă afirmasem în ultima vreme la *Washington Post* ca reporter specializat în criminalitatea informatică și eram nerăbdător să prezint informațiile despre RBN într-un articol care speram să-i facă pe mulți să devină conștienți de dimensiunea amenințării. Credeam cu tărie că membrii comunității criminalității informatice comiseseră o greșeală strategică majoră concentrând atât de mult rău într-un singur loc. Dacă RBN era ostracizată și evitată cumva de restul comunității de pe internet, multe asemenea afaceri aveau să fie deconectate de la web.

Experții în domeniul securității informatice cu care am discutat despre ideea mea au spus că o astfel de acțiune putea crește costurile operațiilor infracționale și le putea îngreuna misiunea găsirii unui „domiciliu" stabil. Aceasta putea duce în cele din urmă la reducerea spamului pentru utilizatorii de zi cu zi și la scăderea numărului siteurilor care răspândesc malware sau comercializează pornografie infantilă. Pentru mine, implicațiile pozitive erau uriașe. Nu numai că aș fi putut reduce sau, eventual, eradica spamul și toți virușii, malwareul și alte probleme de securitate aferente, dar exista și posibilitatea distrugerii unei industrii ilegale, absolut revoltătoare, care face rău copiilor pentru plăcerea perversă a câtorva adulți.

În iunie 2007, am început să bat la cap zeci de persoane în stare să-mi furnizeze date cuantificabile despre activitatea rău intenționată care persista la RBN. În următoarele patru luni, articolul s-a scris aproape de la sine, pe măsură ce datele pe care le primeam din diverse surse despre locația unor siteuri mizerabile, rău intenționate au început să contureze o imagine cu adevărat înfricoșătoare a acestei companii fără scrupule și a activităților acesteia menite să ne supraîncarce rețelele cu e-mailuri nesolicitate.

Acuzații aproape identice s-au putut aduce RBN după analiza datelor incriminatoare primite de la unele dintre cele mai cunoscute companii de securitate din domeniu, printre care Cisco, Dell SecureWorks, FireEye, HostExploit, Marshall/M86, SANS Internet Storm Center, Shadowserver, Sunbelt Software (în prezent GFI), Symantec, Team Cymru, Trend Micro și Verisign, pentru a numi doar câteva.

Ken Dunham, pe atunci director al departamentului de reacție rapidă din cadrul unității de spionaj cibernetic iDefense a companiei Verisign, a declarat că echipa lui a examinat toate proprietățile web găzduite de RBN și nu a putut găsi nici măcar un lucru bun. „Am analizat toate informațiile lor și le-am corelat, spunea Dunham, dar n-am reușit să găsim nimic bun la RBN. Am mai văzut în trecut refugii ale unor grupări infracționale, însă, la acest furnizor, practic totul a fost mereu ilicit sau rău intenționat." Pe scurt, nu exista niciun motiv ca acest ISP să rămână on-line.

Poate din cauza misterului și aureolei de activitate specifică crimei organizate rusești care înconjurau RBN, a fost mult mai greu să conving sursele să spună deschis și clar ce anume știau despre operațiile acesteia. O sursă, un profesor care transmitea zilnic anchetatorilor FBI informații privind vânzarea de pornografie infantilă și alte activități infracționale ale RBN, a declarat că se temea pentru integritatea sa corporală dacă spunea public ce știa.

„Mafia rusească se află în spatele RBN, iar mafioții au arme multe și scrupule puține, a explicat profesorul. Mi-ar plăcea să fiu «expert» pentru tine, dar realmente nu vreau să-mi văd familia ciopârțită."

Era una dintre zecile de afirmații sincere cărora nu le puteam atribui niciodată sursa, iar eu aveam nevoie disperată de experți care să declare oficial ce știau despre RBN, pentru a demasca rețeaua respectivă, care afecta viața a milioane de oameni simpli. După multe insistențe, am determinat

suficienți experți să spună adevărul. Pe 13 octombrie 2007, *Washington Post* a publicat articolul „Shadowy Russian Firm Seen as Conduit for Cybercrime" („Companie rusească obscură considerată principalul canal al criminalității informatice") în prima sa parte și l-a postat la loc vizibil pe siteul propriu.

La scurt timp după aceea, *Washington Post* a mai postat două articole de susținere pe blogul său intitulat „Security Fix", detaliind activitatea rău intenționată a RBN și numind în mod explicit ISP-urile care furnizau RBN conexiuni cu restul internetului. Totul fusese dat în vileag. Acum, după ce numele lor fuseseră dezvăluite, furnizorii respectivi trebuiau să justifice banii primiți de la RBN – o situație imposibilă dată fiind reputația oribilă a RBN, care găzduia orice fel de materiale, oricât de ilegale sau ofensatoare.

În următoarele săptămâni, zeci de mii de adrese de internet atribuite anterior Russian Business Network au fost treptat abandonate. Afacerile ilegale care ocupaseră cândva aceste „parcele" au dispărut, apelând la alți furnizori bulletproof de găzduire web din Italia, China, Coreea și alte țări. Drept urmare, o perioadă scurtă, cât timp botneturile de spam au continuat să expedieze reclame agresive și linkuri către siteuri cu malware, siteurile promovate în acele e-mailuri nu au răspuns. Deși, aparent, a fost o victorie lipsită de importanță, pentru mulți membri ai comunității de securitate ea a reprezentat o lovitură bine-venită, care a avertizat lumea criminalității informatice că industria securității on-line începea în sfârșit să riposteze.

Nu toți erau încântați de ceea ce se întâmpla. Anterior, RBN fusese o concentrare de furnizori de găzduire web cunoscuți, pe care ISP-urile îi puteau bloca sau filtra cu ușurință cu ajutorul unui firewall, pe când, acum, după ce siteurile de la RBN se împrăștiaseră în zeci de rețele, blocarea lor a devenit mai dificilă. ISP-urile trebuiau să-și întindă mai mult plasele de securitate pentru a se asigura că puteau face față siteurilor

rău intenționate, botneturilor și spammerilor. Totuși ISP-urile, autoritățile guvernamentale și corporațiile începeau să acorde în sfârșit atenție acestei lumi subterane a criminalității informatice de care se loveau tot timpul.

Acesta era vârful aisbergului. În august 2008, la aproape un an după ce RBN a fost împrăștiată în cele patru vânturi, am scris o serie de articole despre criminalitatea informatică, concentrându-mă asupra unui ISP dubios numit Atrivo, situat ceva mai aproape de casă. La fel ca McColo, firma creată de tânărul Nikolai, acesta era un furnizor de găzduire din California de Nord care ignorase cererile autorităților și ale comunității de securitate de a deconecta siteurile abuzive care deveniseră sinonime cu găzduirea de botneturi și a unui număr uriaș de siteuri create pentru răspândirea de malware. M-am bazat pe aceleași dovezi strânse de unele companii de securitate care adunaseră date despre RBN, în special pe un raport al celor de la HostExploit, o organizație de profesioniști respectați în domeniul internetului, dedicați cercetării, demascării infractorilor și sensibilizării publicului cu privire la criminalitatea informatică.

Articolele respective, precum și atenția tot mai mare acordată de mass-media și experții în securitate au dus la excluderea treptată de pe internet a lui Atrivo, deoarece partenerii săi din industria ISP care furnizau conexiuni la internet pentru ea și pentru utilizatorii ei au fost discreditați în mod public și, unul câte unul, au rupt legăturile cu firma într-o perioadă de aproximativ două săptămâni.

Unul dintre efectele importante ale închiderii lui Atrivo a fost dispariția rapidă a viermelui Storm, un botnet notoriu care infiltrase și compromisese milioane de PC-uri americane și care „a fost la un moment dat responsabil de expedierea a peste 20% din spam", am spus eu la 17 octombrie 2008, pe blogul „Security Fix" al ziarului *Washington Post*. Atrivo găzduise mai multe servere master pentru viermele Storm, care a lansat ultimul val

de spam cu trei zile înainte ca Atrivo să fie forțată să părăsească internetul de către ultimul ei furnizor de internet rămas.

La o săptămână după închiderea lui Atrivo, am primit o informație de la o sursă de încredere, care avea contacte cu mulți indivizi dubioși din lumea subterană a criminalității informatice. Aceasta mi-a spus că are pentru mine un mesaj din partea unui escroc informatic anonim, care fusese ușor incomodat, dar și impresionat fără să vrea, de ostracizarea organizată a lui Atrivo pe care o începusem eu.

„Spune-i lui Krebs că a făcut o treabă frumoasă cu Atrivo", i-a transmis sursei mele misteriosul infractor. „Dar dacă se gândește să-l atace acum pe McColo, își forțează norocul."

N-am știut ce să înțeleg din mesajul acela, care a părut a fi o observație amuzată, dublată de o amenințare voalată. În momentul în care l-am primit, era însă prea târziu ca să mă mai răzgândesc. Începusem deja de ceva timp o investigație în cazul McColo, ISP-ul condus de Nikolai „Kolea" McColo. Era o evoluție logică, în special pentru că mulți dintre răufăcătorii și botmasterii ale căror operații dubioase, infracționale fuseseră găzduite de Atrivo aveau părți ale infrastructurii proprii găzduite de McColo. Acum, când Atrivo fusese ștearsă de pe internet, McColo devenise un furnizor bulletproof și mai important pentru comunitatea subterană a criminalității informatice.

În după-amiaza zilei de 11 noiembrie, am trimis date strânse pe durata mai multor luni despre detaliile infracțiunilor comise de McColo către cei doi parteneri ISP ai companiei, care o conectau la internet: Global Crossing și Hurricane Electric, ambele cu sediul în SUA. Informațiile au fost prezentate sub forma unei hărți care arăta că serverele utilizate pentru controlul celor mai active cinci botneturi de spam – programe conectate la internet, responsabile de expedierea majorității e-mailurilor nesolicitate din lume – erau găzduite de câteva servere ale unității McColo din California de Nord.

Am bănuit că, după ce avea să li se prezinte istoria activității rău intenționate de acolo, partenerii de internet ai lui McColo vor întrerupe legăturile de afaceri cu furnizorul de servicii de găzduire, paralizându-l efectiv.

După câteva ore, m-a sunat o sursă care urmărea zilnic activitatea globală de spam și care știa că lucram la un articol despre McColo.

— Ce ai *făcut*, Krebs? a întrebat sursa râzând. Abia dacă mai văd vreun spam și se pare că McColo a fost deconectat de la internet!

Nu-mi amintesc să-i fi mulțumit sau să-i fi spus „la revedere" – țin minte doar că am înjurat cu voce tare și am închis repede, ca să sun alte surse pe telefonul mobil. Toate mi-au confirmat aceleași lucru: McColo dispăruse, iar adresa firmei de pe Internet nu putea fi accesată de nicăieri. Misiunea fusese îndeplinită... deocamdată.

Un apel către Benny Ng, directorul de marketing al companiei Hurricane Electric, a dezvăluit motivul. În după-amiaza aceea, ISP-ul întrerupsese legăturile cu McColo.

— Am examinat datele primite de la tine, am văzut amploarea problemei și am spus „fir-ar a naibii!". În mai puțin de o oră, am oprit toate conexiunile cu ei.

La câteva minute după confirmare, am scris și am publicat o postare pe blog despre închiderea lui McColo – care a devenit rapid una dintre cele mai importante relatări din domeniul criminalității informatice, sub aspectul impactului global imediat, până la data respectivă – apoi am început să lucrez la un articol mai lung despre eveniment, care trebuia să apară pe siteul *Washington Post* și, eventual, în ediția „copacilor morți" (cum numeam noi, reporterii de pe internet, cu afecțiune versiunea tipărită) de a doua zi.

Am lucrat de acasă toată noaptea, scriind până când am adormit finalmente în pijama, la tastatura calculatorului, după ce terminasem, în zori.

Articolul a fost publicat pe washingtonpost.com mai târziu, în dimineața respectivă, iar, pentru o scurtă perioadă, a fost unul dintre cele mai populare de pe site în ziua aceea. Asta s-a întâmplat până când o jurist de la washingtonpost.com l-a citit și a explodat pur și simplu. Aparent, nimeni nu ceruse părerea juriștilor; acum ei solicitau ca articolul să fie scos de pe site dacă faptele nu puteau fi confirmate de trei surse, iar unele afirmații despre presupusele activități ilegale ale companiei McColo nu erau nuanțate.

Redactorii de la *Washington Post* și de la alte publicații importante cer în mod obișnuit ca un articol să fie „avizat de juriști" atunci când conține declarații sau afirmații care ar putea crea probleme juridice, mai cu seamă din partea celor numiți în articol, care ar putea formula acuzații de calomnie. Un jurist de la washingtonpost.com n-a acceptat nicio exprimare care măcar să sugereze o activitate ilegală din partea proprietarilor lui McColo, care ignoraseră în mod repetat cererile noastre de a face comentarii. (Pentru a înțelege cât de dubioase erau afacerile de la McColo, singurele puncte de contact de pe siteul companiei erau conturi anonime de mesagerie instantanee.) În fond, nu exista nicio dovadă că cineva asociat cu McColo fusese acuzat de vreun delict. Și atunci de ce afirmam noi asta?

(O precizare importantă: articolul care a fost postat în dimineața respectivă era plin de linkuri către dovezi ale activităților ilegale desfășurate de McColo, care fuseseră strânse de experți din industria securității. Din păcate, jurista de la washingtonpost.com care s-a opus publicării inițiale a citit articolul pe telefonul ei mobil. Acesta eliminase toate hyperlinkurile pe care cititorii le puteau utiliza pentru a vedea rapoarte complexe ale terților și dovezi ale respectivei activități infracționale. Juristei i se părea că în articol erau formulate acuzații neîntemeiate și potențial calomnioase la adresa companiei McColo, a cărei afacere părea a fi distrusă aproape complet în acel moment.)

Jurista a cerut ca articolul despre McColo să fie retras de pe siteul washingtonpost.com și, după o scurtă perioadă de sfidare, biroul de știri al siteului s-a conformat, fără să mă întrebe dacă articolul era corect sau ce dovezi aveam pentru a-l susține. A fost pur și simplu retras de pe site, fără explicații pentru zecile de mii de cititori care au găsit linkuri nefuncționale și, în cele din urmă, au fost redirecționați spre postarea inițială de pe blogul meu. Contul meu de e-mail s-a umplut rapid cu mesaje de la cititorii derutați, care întrebau unde a dispărut articolul.

Timp de aproape cinci ore, urmarea uneia dintre cele mai importante relatări despre criminalitatea informatică de până atunci a rămas în purgatoriul editorial și juridic, deoarece avocații au examinat articolul rând cu rând, schimbând sau ștergând expresii și pasaje potențial inacceptabile.

Articolul a fost republicat până la urmă în seara aceea, deși într-o formă mai scurtă și mult stilizată. Începând din ziua respectivă, orice articol al meu care conținea informații oricât de vagi despre o presupusă activitate criminală on-line trebuia înaintat cel puțin unui redactor de la washingtonpost.com și, adeseori, trecea pe la câțiva juriști. Întrucât pe mine mă interesa criminalitatea informatică, asta se întâmpla de obicei de câteva ori pe săptămână.

După fiascoul cu McColo, reportajele de investigație a căror elaborare dura săptămâni și, uneori, chiar luni puteau să stea tot atât în conturile de e-mail ale superiorilor a căror aprobare trebuia s-o obțin pentru publicare. În unele cazuri, apariția lor a fost amânată pe o durată nedeterminată de redactorii siteului washingtonpost.com sau de juriști.

Pentru unul dintre aceste articole am avut nevoie de șase luni ca să culeg informații și să-l redactez. Era despre o strategie aplicată pentru prima oară de ChronoPay, firma lui Vrublevski. Pe atunci, cel mai folosit și mai profitabil plan de criminalitate informatică din lume era răspândirea de software antivirus fals. Cunoscut ca „scareware", antivirusul fals utilizează alerte

pop-up înşelătoare şi alte trucuri pentru a-i speria pe utilizatorii de internet neavizaţi şi a-i determina să cumpere software de securitate inutil. Colac peste pupăză, programele de securitate false sunt adesea însoţite de malware care transformă computerele-gazdă în zombi de spam.

Experţii în domeniul securităţii care au urmărit îndeaproape flagelul scareware mi-au spus că, în marea majoritate a cazurilor de escrocherie scareware, ChronoPay era responsabilă de procesarea plăţilor cu card de credit şi că fondatorul companiei, rusul Pavel Vrublevski, părea implicat personal în conceperea şi aplicarea acestor planuri.

Am ştiut foarte puţine despre Vrublevski până la sfârşitul anului 2008, când o sursă din Rusia (care va rămâne anonimă) m-a îndemnat să caut documentele de constituire a companiei ChronoPay în Olanda, unde fusese fondată. Ele arătau că firma fusese creată în 2003 în urma unei asocieri în proporţii egale între Vrublevski şi Igor Gusev. Aceeaşi sursă a spus că cei doi s-au despărţit în 2005. În 2006, Gusev a înfiinţat obscura firmă farmaceutică on-line GlavMed–SpamIt. Pentru a nu rămâne în urmă, un an mai târziu, Vrublevski avea să fie cofondator al companiei Rx-Promotion, o altă farmacie ilicită de pe internet.

În acel moment, nu aveam nicio idee despre legăturile lui Vrublevski cu Rx-Promotion. Nu ştiam nici măcar cine era Igor Gusev. Ştiam doar că ChronoPay fusese asociată recent cu viermele Conficker, una dintre cele mai virulente şi examinate tulpini de malware create vreodată. O primă versiune a viermelui instruise milioane de computere infectate să descarce un program antivirus periculos de la Trafficconverter.biz, o afacere on-line care a câştigat zeci de milioane de dolari plătind spammeri pentru a băga pe gâtul utilizatorilor de PC-uri software antivirus fals. ChronoPay a fost compania responsabilă de procesarea plăţilor către TrafficConverter.

În martie 2009, am terminat de scris prima versiune a unui articol în care dezvăluiam rolul central jucat de ChronoPay în

răspândirea programelor antivirus false. În articol prezentam, de asemenea, dovada că Vrublevski era fondatorul, proprietarul și creatorul lui Crutop.nu, obscurul forum on-line dedicat spammerilor și escrocilor care fuseseră martori la dispariția companiei McColo.

Citam în articol studii ale unor experți în domeniul securității despre activitatea firmei ChronoPay. Cu toate acestea, redactorii washingtonpost.com l-au pasat unul altuia vreme de câteva luni, fiind convinși că ChronoPay va acționa în judecată *Washington Post*, ceea ce era de înțeles. În discuția noastră telefonică, Vrublevski promisese că firma lui avea să facă exact acest lucru dacă publicam articolul.

Aceeași șovăială a întârziat difuzarea unei alte știri importante legate de articolul despre ChronoPay. Când McColo a fost închisă, mare parte din activitatea sa ilegală a fost transferată repede unui alt furnizor de găzduire din California de Nord, Triple Fiber Networks sau 3FN, cum era cunoscut în subteran. Aceiași operatori de botneturi de spam care fuseseră găzduiți câțiva ani de McColo au început să folosească 3FN după dispariția acesteia. O trecere în revistă a postărilor de pe forumul on-line Spamdot – un bârlog bine păzit al răufăcătorilor, în care, la vremea respectivă, se adunau majoritatea spammerilor ruși – a arătat că proprietarii 3FN i-au preluat pe clienții lui McColo când operațiunile companiei au fost închise în noiembrie 2008.

În acel moment, 3FN era cel mai mare serviciu de găzduire de siteuri care promovau agresiv programe antivirus false. Siteul 3FN era ciudat de asemănător cu cel al firmei McColo. De asemenea, singura modalitate de a-i contacta pe proprietarii companiei era ICQ („I seek you"/„Te caut eu"), un protocol de mesagerie instantanee care era de ani de zile mediul de comunicare *de facto* pentru mulți hackeri ruși.

Am insistat ca toate aceste lucruri să iasă la lumină. După ce am dezvăluit activitatea rău intenționată care a scos până

la urmă de pe piață firmele RBN, Atrivo și McColo, am crezut că *Washington Post* are, față de cititorii săi – și față de lumea întreagă – obligația de a menține reflectoarele ațintite asupra acelor furnizori de internet care ofereau adăpost unei părți uriașe a comunității criminalității informatice. Comentariile apărute în principalele publicații care condamnau aceste companii ar fi determinat mai multe autorități să ia măsuri împotriva lor și ar fi redus astfel amenințarea pe care o reprezentau atât pentru americani, cât și pentru oamenii din toată lumea. Redactorii mei însă n-au vrut să repete povestea cu McColo, deși aceasta nu crease probleme de ordin juridic sau de altă natură ziarului *Washington Post*.

Când am menționat, la o ședință de redacție de la începutul anului 2009, că 3FN era anchetată pentru infracțiuni cibernetice de autoritățile americane în domeniu, s-a insistat ca, înainte de a publica orice articol despre presupusele nereguli de la 3FN, să obținem confirmarea faptului respectiv din minimum două surse sau să așteptăm comentariul oficial cu privire la anchetă ori dovezi ale punerii sub acuzare a furnizorului de servicii de găzduire. Documentele referitoare la acest caz fuseseră sigilate de un judecător federal, iar sursa mea din agenția care făcea ancheta era singura care auzise vreodată de 3FN. Articolul a fost oprit momentan de la publicare.

Apoi, la 2 iunie 2009, peste 15 000 de siteuri găzduite de 3FN au fost dezactivate după ce Comisia Federală pentru Comerț (FTC) din SUA a convins un judecător din California de Nord să-i oblige pe furnizorii de internet din amonte să nu mai direcționeze traficul pentru 3FN. Comisia a susținut că 3FN opera „ca furnizor de servicii de internet «dubios» sau «black hat», care recruta, găzduia cu bună știință și participa activ la distribuirea de conținut ilegal, rău intenționat și dăunător", inclusiv servere de control al botneturilor, pornografie infantilă și produse antivirus îndoielnice.

Măsura luată de FTC mi-a oferit elementul de siguranță necesar pentru a găsi până la urmă sprijin în continuarea anchetei despre Vrublevski, ChronoPay și rolul lor în dezvoltarea pieței de antiviruși falși, care afecta milioane de consumatori și le amenința identitatea, finanțele și securitatea. Crutop.nu a fost, de asemenea, găzduit de 3FN, fiind chiar amintit în măsura luată de FTC, care l-a numit un loc „în care infractorii își comunică tehnici și strategii" și un site de limbă rusă „care conține o mulțime de forumuri de discuții axate pe obținerea unor câștiguri bănești din spam". Examinarea mai multor fire de discuții de pe forumul rus dedicat webmasterilor de pornografie a indicat că cei peste 8 000 de membri activi ai Crutop alcătuiseră cea mai mare bază de clienți ai lui 3FN.

Este edificator faptul că, imediat după ce 3FN a fost închis – dar înainte ca siteul washingtonpost.com să publice articolul despre legăturile lui ChronoPay cu industria antivirușilor falși – pagina de pornire a lui Crutop.nu a fost schimbată cu o lungă tiradă despre măsura luată de FTC împotriva 3FN. Acela avea să fie primul meu contact cu interminabilele diatribe ale lui Vrublevski. O parte din mesajul respectiv suna așa:

> În concluzie, am dori să adăugăm că, deși paragraful 1 al regulilor noastre n-a fost luat niciodată în serios până acum și a fost scris ca o glumă, legat de evenimentele recente, am dori totuși să știm cum a fost posibil ca nu mai puțin de cinci (5!) experți-agenți reputați (printre care specialiști NASA și dl Brian Krebs) din SUA (unde fiecare a zecea persoană vorbește limba rusă, sursa: Wikipedia) să nu-și dea seama că, pe Crutop.nu, în subforumul SPAM, discuțiile n-au nicio legătură cu spamul sau cu alte infracțiuni informatice?

Articolul despre Vrublevski și rolul-cheie jucat de ChronoPay în 3FN a fost publicat până la urmă după mai bine de patru luni de la predare. Nu a urmat niciun proces din partea lui Vrublevski sau ChronoPay, însă redactorii de la *Washington Post* au declarat că sunt profund îngrijorați de preocuparea mea

pentru băieții răi de pe internet. Șefii ziarului erau neliniștiți fiindcă scriam despre un subiect în legătură cu care nu există în mod obișnuit dovezile documentare clasice. De asemenea, ei considerau că interesul meu pentru criminalitatea informatică – spre deosebire de un domeniu mai larg, ca tehnologia de larg consum sau politica tehnologică – era prea îngust și că mă apropiam prea mult de sursele mele pentru a-mi păstra obiectivitatea.

Le-am împărtășit preocupările... într-o oarecare măsură. Niciun jurnalist nu vrea să depindă de câteva surse și să le excludă pe altele; dacă procedează așa, riscă să publice articole fără perspectivă și echilibru. Știam însă că, în cazul acesta, aveam nevoie de surse mai multe și mai bune – în special dintre cele implicate activ în comunitatea criminalității informatice. De asemenea, eram convins că subiectul „3FN" era prea important pentru a nu fi abordat mai departe și că abandonarea lui ar fi însemnat ratarea unei șanse de a dezvălui – și, eventual, de a stopa – o mare parte din activitatea legată de criminalitatea informatică.



La o ședință de la jumătatea anului 2009, redactorii de la washingtonpost.com au explicat că, deși blogul meu, „Security Fix", atrăgea extraordinar de mulți cititori loiali, ținând cont de subiectul de nișă, punctul de vedere exprimat în articolele mele nu se încadra în strategia de viitor a ziarului *Washington Post*, de a fi principala sursă de informații „pentru și despre Washington, DC".

Această expresie rezuma noua strategie care era componenta principală a unui efort îndelungat și susținut de a unifica operațiunile separate ale ziarului *Washington Post* cu redacția siteului washingtonpost.com, în special din motive de cost.

Conducerea ziarului ajunsese la concluzia că o modalitate de a economisi bani era să schimbe orientarea ziarului și a siteului, astfel încât acestea să se concentreze asupra evenimentelor din capitala țării și să explice cititorilor în ce fel

evenimentele de la Washington afectau restul lumii. S-a optat, de asemenea, pentru închiderea unora dintre birourile majore din SUA și folosirea într-o măsură mai mare a serviciilor unor agenții de presă ca Associated Press și Reuters, pentru informațiile de ultimă oră.

Redactorii sperau să scriu mai mult despre politica tehnologică, în special despre reglementările din domeniul tehnologiei, sau despre viitorul inovației tehnologice în raport cu politica tehnologică. Eu însă nu doream să nu mai scriu despre criminalitatea informatică. Mă ocupasem de politica tehnologică vreme de câțiva ani, la începutul carierei mele la *Washington Post,* și consideram tema respectivă plictisitoare și banală.

Revenirea la politica tehnologică ar fi însemnat, de asemenea, abandonarea celor patru ani în care îmi făcusem relații cu surse informate, care aveau legături atât în industria de securitate, cât și în comunitatea criminalității informatice. Scriam de un an despre atacurile informatice tot mai costisitoare și mai sofisticate, lansate în fiecare lună împotriva a nenumărate organizații mici și mijlocii din toată țara. După toate cercetările și investigațiile făcute, ajunsesem în sfârșit să-mi fac o imagine despre activitățile zilnice ale marilor bande de infractori informatici care operau din Europa de Est.

În câteva luni, reușisem să aflu cine erau acei infractori, unde lucrau, ce făceau în timpul liber și pe cine atacau – adesea, înainte ca victimele însele să știe că fuseseră jefuite de sute de mii, uneori de milioane de dolari. Conturile bancare ale majorității organizațiilor și firmelor mici sunt gestionate de oameni obișnuiți, care nu fac față grupărilor de crimă organizată care operează pe internet, și doream cu disperare să scriu mai departe despre această formă de jaf on-line, tot mai practicată și mai costisitoare.

Mai mult, începeam să înțeleg că Vrublevski și ChronoPay erau de fapt vârful aisbergului – că erau doar cele mai vizibile

figuri ale unei comunități subterane, concentrate în Rusia și Europa Răsăriteană, ai cărei membri păreau să se cunoască între ei și să se bazeze pe unul pe altul.

Astfel, după 14 ani de muncă la *Washington Post*, am fost lăsat să plec după ce mi s-a plătit salariul pe șase luni, timp suficient pentru a-mi plănui următoarea mișcare în carieră. Îmi amintesc că, în acel moment, era foarte important pentru mine să-mi găsesc un nou loc de muncă până la 1 ianuarie 2010. Nu eram totuși sigur care avea să fie noua mea îndeletnicire.

Nu am discutat despre plecarea de la *Washington Post* decât cu câțiva membri ai familiei și cu două surse de încredere, cu nimeni altcineva. De aceea, am fost surprins când, după nici o lună și cu mult înainte de data încetării oficiale a activității mele la *Washington Post*, am descoperit pe Crutop.nu un lung fir de discuții având titlul „Krebs concediat de la *Washington Post*", în care membrii forumului își exprimau satisfacția în legătură cu acest lucru.



„Pentru aceia dintre voi care nu știu – el este autorul lui Security Fix de la WP, căruia îi plăcea să scrie despre Atrivo, McColo, EstDomains, UkrTeleGroup și 3FN și care a ajutat la închiderea lor", a scris membrul Crutop care a deschis firul de discuții. Alții au salutat știrea astfel: „Mulțumesc, Moș Crăciun!" sau „Moș Crăciun a primit scrisorile noastre!" A fost straniu și deranjant să văd că ceva atât de personal era expus pe un forum public, administrat de unii dintre cei mai activi spammeri pe care mă străduiam să-i demasc, dar acele reacții m-au determinat să-mi continui munca.

Cu doar două săptămâni înainte de postarea pe Crutop a firului respectiv de discuții, înregistrasem fără să știe nimeni numele de domeniu KrebsOnSecurity.com, dar încă nu hotărâsem dacă să caut un loc de muncă la altă publicație majoră ori să continui singur să realizez un blog. După cele auzite de la colegii din alte instituții mass-media importante, care fuseseră forțați să-și ia concediu fără plată sau cărora li se

dăduseră rubrici care atrăgeau mai multă publicitate, nu eram nerăbdător să revin la un ziar sau la o publicație on-line importantă. Totuși ideea de a lucra pe cont propriu – și de a-mi câștiga existența astfel – mi se părea descurajatoare, uneori chiar îngrozitoare.

În același timp, voiam să reușesc în condițiile impuse de mine și să-mi fac un public bazându-mă exclusiv pe reportajele mele originale. Când am citit discuțiile de pe Crutop, am luat-o aproape ca pe o provocare personală și am decis s-o accept. Ce m-a încurajat a fost faptul că, în scurt timp, am primit mesaje de la mai mulți cititori ruși care își exprimau dezgustul față de acele discuții și erau nerăbdători să pună la dispoziție documente care puteau dovedi amploarea implicării lui ChronoPay în criminalitatea informatică subterană. Bănuiam, dar nu puteam fi sigur în momentul acela, că în spatele acestei stratageme se afla Igor Gusev, fostul partener de afaceri al lui Vrublevski – devenit între timp dușman de moarte al acestuia – dar pentru moment nu voiam să fac nimic care să descurajeze sursele să-mi spună ceea ce știau.

„Nu te lăsa păcălit", a subliniat într-un e-mail o sursă care folosea pseudonimul „Boris" și care promisese să-mi transmită numeroase dovezi incriminatoare despre infracțiunile săvârșite la ChronoPay. „Tipii ăștia, și probabil Vrublevski, te vor ataca și s-ar putea să fie destul de neplăcut."

Boris și alții s-au ținut însă de promisiunile făcute, iar avertismentele lor s-au adeverit. Amenințările anonime au început la doar câteva zile după ce am primit o mulțime de e-mailuri și documente care îi incriminau pe cei de la ChronoPay. Atunci a dispărut și ultima ezitare pe care o mai avusesem în privința muncii pe cont propriu. Era timpul să mă apuc de treabă.

# Capitolul 3

# RĂZBOIUL FARMA

Dimineaţa zilei de 14 mai 2010 a început cu un mesaj incoerent şi neliniştitor, care aştepta în contul de e-mail. Autorul anonim îmi citise postarea de pe blog despre o prelegere publică privind criminalitatea informatică pe care tocmai o susţinusem la New York. Mesajul suna astfel:

> Brian,
>
> Eşti o extraordinară enigmă. Se pare că soţia Îţi îngăduie să Te comporţi ca un adolescent. Aş vrea să văd că Te maturizezi.
>
> Noi Te iubim. Dar soţia Ta are dreptate. Este timpul să pui talentul special pe care îl ai în slujba profesioniştilor. Ultima relatare despre deplasările Tale în nordul New Yorkului mă sileşte să-ţi transmit această rugăminte finală înainte ca...
>
> Soţia Ta, care suferă de atâta timp, dar Te iubeşte, ar trebui să fie împuternicită să încheie un contract cu un profesionist (care ar putea fi o femeie, dar docila Ta soţie i-ar mânca ochişorii cu cerealele de la micul dejun dacă s-ar da la Tine).
>
> Deci de ce-ţi scriu? Păi, e simplu. Îmi place ce faci şi multor altora le-ar plăcea dacă ar şti despre Tine. Dar, la fel ca mulţi artişti, Tu crezi că toţi văd ceea ce vezi Tu. Noi nu vedem.
>
> De aceea, următoarea mişcare depinde de Tine. Aş începe cu soţia Ta. Aş întreba-o ce crede ea despre acest e-mail.
>
> Apoi, mi-aş lua un avocat. O să ai nevoie de unul când ea se va „îndrăgosti".

Mesajul era în stilul lui Vrublevski: răutăcios, incoerent, plastic şi plin de tot felul de metafore. Era genul de mesaj pe

care îl vedeam frecvent la „RedEye", presupusa identitate a lui Vrublevski de pe Crutop.nu – forumul rusesc dedicat webmasterilor de pornografie la crearea căruia luase parte și care era un centru educațional pentru spammeri. Așa cum l-a descris Comisia Federală pentru Comerț în momentul închiderii furnizorului de servicii de găzduire 3FN, Crutop „conține o mulțime de forumuri de discuții care se concentrează pe obținerea unor câștiguri bănești din spam".

Încă de la începutul activității sale, Vrublevski își făcuse un renume creând o rețea de siteuri pentru adulți specializate în pornografie extremă și violentă, mai ales videoclipuri cu violuri, incesturi și zoofilie. Numele lui și adresa ChronoPay se află pe documentele de constituire ale firmei „Red & Partners BV", creată de Vrublevski, compania-mamă a programului de afiliere dedicat webmasterilor de pornografie, conform documentelor legale obținute de autor de la statul olandez. De asemenea, după cum am menționat într-un articol publicat în 2009 în *Washington Post*, siteurile ChronoPay.com și Red & Partners (re-partners.biz) împărțeau aceleași servere de nume de domeniu și același cod Google Analytics pentru urmărirea vizitatorilor siteului, deși ChronoPay a negat orice legătură între cele două. Mulți webmasteri de pe Crutop erau afiliați care câștigau bani din revânzarea abonamentelor la siteuri porno administrate de Vrublevski și de alte persoane de pe forum.

Pe lângă limbajul ciudat și oarecum amenințător, mesajul conținea câteva indicii care-mi confirmau bănuiala că fusese scris de Vrublevski. Deși era doar o suspiciune, momentul ales dădea de bănuit.

Cu șase luni în urmă, decisesem să lucrez pe cont propriu și să-mi încep propriul site – KrebsOnSecurity.com – un blog de știri zilnice, dedicat investigațiilor privind criminalitatea informatică, menit să sporească gradul de conștientizare a publicului și să determine luarea unor măsuri de combatere a fenomenului. E-mailul sosise la numai două zile după ce-i

spusesem lui Vrublevski că mă pregăteam să public un articol bazat pe acuzațiile aduse lui de Ilia Ponomarev, deputat, membru al Comisiei de dezvoltare tehnologică a Dumei de Stat din Rusia. Ponomarev trimisese o scrisoare anchetatorilor ruși, reproducând multe dintre acuzațiile formulate în reportajele mele anterioare publicate în *Washington Post* despre ChronoPay și Vrublevski.

Scrisoarea lui includea, de asemenea, o informație necunoscută mie, care mi-a oferit primul dintre multele indicii privind corupția pe scară largă din politica rusă. În mod incredibil, Vrublevski – care, potrivit multor surse, conducea unul dintre cele mai cunoscute programe de spam farmaceutic, Rx-Promotion – fusese ales președinte al grupului de lucru antispam de la Ministerul Telecomunicațiilor și Comunicării în Masă, un organ creat de președintele rus Dmitri Medvedev pentru a consilia guvernul cu privire la noile legi destinate reducerii volumului de e-mailuri nesolicitate. În principiu, Ponomarev dorea plecarea lui Vrublevski.

Când l-am contactat pentru comentarii cu privire la scrisoarea lui Ponomarev, Vrublevski a negat public asocierea cu Rx-Promotion sau cu spamul, după care m-a acuzat că am fost mituit de dușmanii săi pentru a crea o imagine negativă despre el în presă. A promis din nou că mă va da în judecată și chiar a făcut pași concreți în această direcție. În momentul discuției noastre, el începuse deja acțiunea în instanță, dar, după cum am aflat, avocatul lui și directorii de la ChronoPay l-au convins să renunțe, pentru că șansele de câștig erau slabe, iar acțiunea s-ar fi putut prelungi ani de zile, timp în care el și ChronoPay ar fi devenit vulnerabili, căci multe dintre activitățile lor ar fi fost aduse la lumina zilei dacă procesul ar fi început efectiv.

Cum am aflat eu toate astea când Vrublevski n-a spus niciodată nimic, cu excepția faptului că m-a amenințat cu judecata? În momentul respectiv, în contul meu de e-mail au început să se „scurgă" zeci de e-mailuri, care fuseseră transmise între Vrublevski și un avocat vorbitor de limbă rusă angajat de el de

la firma de avocatură Duane Morris LLP din Washington, DC. E-mailurile aveau să arate ulterior că, pentru a mă reduce la tăcere, Vrublevski fusese pregătit să plătească peste 100 000 de dolari ca să mă dea în judecată pentru calomnie, pentru postările mele despre rolul jucat de el în industria antivirușilor și a farmaciilor ilicite.

Acele e-mailuri interne au fost primele dintre numeroasele materiale compromițătoare (*kompromat,* cum sunt numite în Rusia) pe care aveam să le primesc în decursul unui an de la hackeri anonimi, aparent decișiși să-i demaște pe cei de la ChronoPay și pe Vrublevski. Când am început să primesc materialele acestea – de obicei prin intermediul unui link spre o arhivă de pe un site de partajare gratuită a fișierelor – am analizat și posibilitatea ca e-mailurile și documentele să fi fost falsificate pentru a le face să pară furate de la ChronoPay. În cele din urmă însă, volumul, complexitatea și legăturile dintre ele au arătat clar că erau autentice.



După câteva luni, Vrublevski însuși avea să recunoască asta față de mine într-o conversație telefonică. Hackeri necunoscuți sau persoane din interiorul firmei ChronoPay făcuseră să se scurgă în mediul on-line un volum uriaș de corespondență internă – zeci de mii de e-mailuri și documente contabile – precum și sute de ore de conversații telefonice pe care Vrublevski le înregistrase cu alții. Informațiile dovedeau amploarea implicării ChronoPay în afaceri dubioase cu farmacii și antivirușifalși. Acestea presupuseseră crearea unei rețele complexe de companii-paravan și conturi bancare offshore – toate fiind înregistrate în documente Excel și, în unele cazuri, descrise chiar de Vrublevski cu gura lui.

Acest adevărat tezaur conținea nu numai dovezi ale ilegalităților comise de ChronoPay și de directorii săi, ci și detalii complicate, uneori sinistre, despre unii dintre cei mai puternici oameni din lumea subterană a criminalității informatice.

A durat multe luni să citesc toate materialele și, mai important, să descopăr cele mai importante e-mailuri și documente.

Greutățile au fost cauzate de faptul că, în mod paradoxal, chiar căsuțele de e-mail ale angajaților ChronoPay la care mi se oferise acces off-line erau pline de spam, dând o mulțime de rezultate fals pozitive când am căutat în ele termeni specifici care puteau dezvălui implicarea ChronoPay în constituirea de companii-paravan și programe de afiliere, ca și în desfășurarea de operații spam. De asemenea, aproape toate mesajele erau scrise în rusă, iar expresii specifice sau substantive proprii conțineau adesea permutări ale echivalentelor chirilice, transliterate în rusă, ori erau prescurtări ce necesitau căutări individuale sau și una, și alta.

Din fericire, cu patru ani înainte, începusem să învăț singur limba rusă. Pe când lucram la *Washington Post*, descoperisem că petreceam foarte mult timp pe forumuri rusești, care nu numai că erau ostile occidentalilor, ci, de cele mai multe ori, îi pedepseau sau îi suspendau pe membrii lor pentru păcatul de neiertat de a comunica în engleză. Pentru a depăși acest obstacol, am împrumutat de la biblioteca locală CD-uri care conțineau 60 de ore de lecții de limba rusă. Până în 2008, reușisem să învăț destul de bine rusește pentru a putea citi majoritatea forumurilor fără ajutorul unui serviciu de traducere on-line. Pentru un reporter de investigații ca mine, a fost vital să mă asigur că nu interpretam greșit niciuna dintre informațiile pe care le preluam de acolo. În plus, mi-a fost mult mai ușor să fac cercetări.

Examinând documentele, am descoperit sute de e-mailuri între Vrublevski și Stanislav Malțev, fost anchetator în cadrul Ministerului de Interne rus. În 2007, Malțev se ocupase de investigarea acuzațiilor de afaceri ilegale la adresa lui Vrublevski. În scurt timp însă, Vrublevski l-a angajat pe Malțev ca șef al securității sale, iar acțiunea pornită împotriva lui a murit încă din față.*

* Vrublevski a afirmat că acuzațiile erau false, nefiind altceva decât un șantaj orchestrat de dușmanii săi, dar compania care era „șantajată" lucra cu o monedă virtuală pe care o crease el pentru a-i

A devenit de asemenea clar că directorii firmei ChronoPay încercaseră în zadar să izoleze proiectele „negre" ale companiei – de exemplu, programul de spam farmaceutic Rx-Promotion și afacerea cu antivirușii falși – de baza de clienți legitimi. E-mailurile scurse de la ChronoPay arată că, în august 2010, cofondatorul Pavel Vrublevski a autorizat o plată de 37 350 de ruble (aproximativ 1 200 de dolari) în schimbul unei licențe multi-user pentru un serviciu de urmărire și gestionare on-line a proiectelor numit MegaPlan.

Angajații ChronoPay își foloseau conturile MegaPlan pentru a urmări problemele legate de procesarea plăților, volumul comenzilor făcute de clienți și parteneriatele publicitare pentru aceste programe „negre". Inspirându-se parcă din filmul *Reservoir Dogs* al lui Quentin Tarantino, angajații au adoptat pseudonime ciudate ca „Mr. Kink", „Mr. Stranger", „Mr. Templar" și „Ms. Gandalfine".



Cu toate acestea, într-un caz clasic de eșec de securitate operațională, mulți dintre acești angajați și-au trimis în mod automat mesajele și parolele MegaPlan în conturile proprii de e-mail de la ChronoPay, care au ajuns astfel în e-mailurile scurse. O organigramă de pe pagina de pornire a siteului MegaPlan ChronoPay arăta că fostul polițist Malțev (alias Mr. Heppner) fusese numit manager adjunct la Rx-Promotion, deasupra lui fiind doar „big boss", Vrublevski (alias RedEye).

Aveam în sfârșit cheia pe care o căutasem. Conturile MegaPlan ofereau cele mai multe informații privind gradul de implicare a ChronoPay în dezvoltarea pieților de antivirușii falși sau „scareware". Acestea sunt programe care emit alerte false de securitate despre amenințări inexistente pe PC-ul victimei și apoi preiau controlul computerului până când victima fie găsește o modalitate de a elimina malwareul, fie cumpără un software fals.

---

ajuta pe webmasterii și spammerii proprii să fie plătiți fără a lăsa urme în rețelele bancare rusești.

Aceste tipuri de programe afectează zeci de milioane de oameni din toată lumea și sunt extraordinar de profitabile. Majoritatea utilizatorilor de computere n-ar putea să spună că n-au întâlnit niciodată un asemenea mesaj, care este doar semnul cel mai vizibil că PC-ul respectiv a fost atacat de un spammer sau de alte programe malware ascunse. (Indiferent cum ați proceda, nu dați niciodată clic pe aceste mesaje! Încercați să eliminați imediat malwareul cu ajutorul unui antivirus profesional sau consultați epilogul acestei cărți pentru a afla ce puteți face ca să nu înrăutățiți și mai mult o astfel de situație nefericită.)

Informațiile scurse arată că divizia de „proiecte negre" sau de mare risc a ChronoPay a lucrat intens pentru a rămâne în vârful industriei scareware. În martie 2010, compania a început să proceseze plățile pentru icpp-online.com, un site inovator de escrocherii, care fura banii victimelor forțându-le să plătească „o sumă anteprocesuală" drept „amendă pentru încălcarea dreptului de copyright".

Așa cum au observat în momentul respectiv cei de la compania de securitate F-Secure, victimele acestei escrocherii erau informate că „o scanare făcută de Antipiracy Foundation" găsise pe computerul lor fișiere cu muzică și filme piratate și că cei care refuzau să plătească 400 de dolari folosind cardul de credit riscau pedeapsa cu închisoarea și amenzi uriașe. Planul era extraordinar de simplu. La un moment dat, mulți oameni au privit ori au ascultat materiale piratate, astfel încât nu exista niciun motiv pentru ca ei să nu creadă mesajul respectiv. Drept urmare, mii de utilizatori au fost înșelați.

Marea șmecherie fusese următoarea: de mulți ani, programele scareware reprezentau o problemă numai pentru utilizatorii care navigau pe internet folosind computere ce rulau sistemul de operare Windows de la Microsoft. În mai 2011 însă, furnizorii de scareware au început să vizeze pentru prima dată

utilizatori ai sistemului de operare Mac OS X de la Apple. Din acel moment, nimeni nu a mai fost ferit de spam și atacuri malware.

Documentele interne scurse de la ChronoPay aveau să dezvăluie rolul jucat de companie în această inovație. La câteva zile după primele atacuri, utilizatori experimentați de Mac de pe forumurile de asistență Apple au început să raporteze că noi tulpini ale acestui malware de Mac îi puneau pe utilizatori să plătească programul printr-un domeniu numit mac-defence.com. Alții au detectat software de securitate Mac fals, care provenea de la macbookprotection.com. Când am examinat pentru prima oară documentele de înregistrare ale acelor domenii, nu m-a surprins să găsesc amprenta distinctă a celor de la ChronoPay.



Documentele de înregistrare a siteurilor pentru ambele domenii includ adresa de contact fc@mail-eye.com. Potrivit documentelor sustrase de la ChronoPay, firma deținea domeniul mail-eye.com și plătise pentru serverele virtuale din Germania pe care rula acesta. Ele indicau și că adresa fc@mail-eye.com aparținea controlorului de gestiune al lui ChronoPay, care era pe atunci o persoană numită Aleksandra Volkova. Una dintre dovezile irefutabile fusese găsită și era momentul să informez publicul.

După publicarea articolului despre Ponomarev, am început să primesc telefoane de la Vrublevski cel puțin o dată pe zi, adesea fără un motiv aparent. Apelurile proveneau aproape de fiecare dată de la alt număr. (Când l-am întrebat de ce apelurile lui păreau să provină mereu de la alt număr de telefon rusesc, Vrublevski a răspuns cu nonșalanță că avea în acel moment nu mai puțin de nouă telefoane mobile și că aceasta era o tactică uzuală a afaceriștilor ruși de succes care doreau să scape de supravegherea agenților guvernamentali indiscreți.)

La început, am crezut că dramatiza sau că era paranoic; mai târziu, aveam să aflu că era într-adevăr ținta supravegherii statului rus. „Gusev a menționat pe blogul lui numele unui tip din FSB care lucrează la cazul Vrublevski, mi-a spus directorul executiv al ChronoPay într-o convorbire telefonică, vorbind despre sine la persoana a treia. Ei mi-au interceptat convorbirile telefonice și știu că discutăm frecvent."

Am descoperit repede că era un individ căruia îi plăcea să-și audă vocea ca nimeni altuia dintre toți cei pe care i-am cunoscut vreodată. În ciuda a tot ceea ce știam despre el – și a faptului că era adesea extraordinar de vulgar și sarcastic, iar de multe ori de-a dreptul insultător – l-am găsit de asemenea dezarmant de fermecător, amuzant și plăcut. Îi plăcea să râdă de el însuși așa cum râdea de alții și avea o mulțime aparent nesfârșită de povești despre persoane influente, politicieni și escroci informatici ruși. Fără să i se sugereze, Vrublevski trecea cu entuziasm de la o poveste pitorească la alta, ca și cum ar fi povestit o telenovelă complicată, dar care nu părea să aibă niciodată o intrigă sau un final.

Moscova este cu opt ore înaintea fusului orar al Washingtonului, astfel încât Vrublevski mă suna de obicei când șoferul îl aducea acasă de la sediul ChronoPay. Pe scurt, era frecvent dispus să se relaxeze și să flecărească tocmai când eu mă pregăteam să-mi încep ziua de muncă. Majoritatea conversațiilor se încheiau în momentul în care eu închideam telefonul fiindcă el nu înțelegea că aveam lucruri mai importante de făcut decât să-l ascult bătând câmpii ore în șir.

Inițial, am crezut că scopul apelurilor telefonice era să mă determine să public ceva care să-l exonereze de infracțiunile săvârșite, din care descopeream zilnic tot mai multe. În toate discuțiile noastre, Vrublevski avea mare grijă să se prezinte ca un luptător împotriva criminalității informatice, hotărât să distrugă industria de spam și să ajute la arestarea și condamnarea tuturor spammerilor.

Vrublevski insinua întruna că eu nu aveam habar de criminalitatea informatică și că nu exista nicio modalitate de a înțelege pe deplin acest subiect dacă nu făceam cel puțin o vizită în Rusia. Într-o conversație, s-a oferit să-mi plătească avionul până la Moscova ca să pot vedea cu ochii mei că, de fapt, el era unul dintre băieții buni.

„Îți propun să vii la Moscova, iar dacă n-ai bani... Îmi dau seama că jurnaliștii nu sunt așa bogați în America... Vom fi încântați să achităm noi toate cheltuielile", a spus Vrublevski într-o conversație telefonică, la 8 mai 2010.

Când am refuzat politicos invitația, a râs și mi-a spus că greșeam dacă mă consideram mituit sau intimidat (adică exact așa cum mă simțeam).

„E amuzant să crezi că, dacă vii să ne întâlnim la Moscova sau la sediul ChronoPay, ești în pericol să fii omorât, a spus el, parcă citindu-mi gândurile. Vino la Moscova și convinge-te cu ochii tăi. Ia-ți notebookul, vino la biroul meu. Stai în fața mea și privește în jur. Pentru că tu primești informații care, ca să fiu sincer, nu sunt reale." (În cele din urmă, aveam să fac exact așa cum m-a îndemnat Vrublevski, după cum vom vedea în capitolul 9, „Întâlnire la Moscova".)

După aproximativ o lună în care am vorbit la telefon zilnic cu Vrublevski – uneori și de două ori pe zi – mi-am dat seama că îmi oferea informații parțial demne de încredere despre alți escroci informatici în speranța că mă voi documenta și voi scrie despre ei, nu despre el.

Problema reală a acestor conversații – în afară de faptul că îmi ocupau jumătate din ziua de lucru – era găsirea frânturilor de adevăr în cugetările lui Pavel, în teoriile lui paranoice cu privire la existența unei conspirații și în încercările de a-mi abate atenția de la propriile sale acțiuni. Când l-am întrebat direct ce credea despre teoria mea – conform căreia încerca să-mi abată atenția de la el însuși, fermecându-mă cu povești complicate despre afaceriști rivali din lumea

interlopă rusă – a lăsat telefonul din mână, râzând în hohote timp de aproape un minut.

„Știi, Brian, câteodată mă surprinzi. Realmente. De-aia te iubesc, să fiu al naibii, a spus el după ce și-a luat telefonul, râzând zgomotos și amuzându-se în continuare pe seama mea. De ce spun asta? Să știi că, uneori, nu-s tocmai sigur că ești foarte isteț. După care, vii cu câte o chestie de-asta. Da, Krebs, uneori ești mult mai isteț decât pari."

Dar Vrublevski putea fi și exploziv, predispus la schimbări bruște de dispoziție și la accese de furie, cu bâlbâieli și înjurături. Alteori, vocea de la celălalt capăt al liniei părea să aparțină unei persoane complet diferite, având un ton scăzut și fiind relativ liniștită. Adesea, asta se întâmpla noaptea târziu, când cei trei copii și soția lui, Vera, erau deja în pat, iar el băuse probabil ceva sau recursese la alte mijloace pentru a se destinde.

În timpul unei lungi convorbiri telefonice, la scurt timp după ce l-am informat că am primit *kompromatul*, Vrublevski era prost dispus și mi-a oferit destul de direct 30 000 de dolari ca să-i predau toate materialele pe care le primisem. Îi povestisem despre documentele scurse, pentru că bănuiam că știa deja destul de bine ce informații ajunseseră pe internet. În mod evident, era mai interesat să-mi cumpere tăcerea pe viitor decât să recapete *kompromatul*. Am refuzat politicos oferta și i-am spus că, deși eram măgulit, intenționam să-mi continui investigațiile.

În scurt timp, am înțeles că Vrublevski avea în minte o altă țintă, mult mai importantă, în această adevărată cruciadă purtată pentru recâștigarea imaginii pozitive a lui ChronoPay: Igor Gusev, fostul lui partener de afaceri de la ChronoPay, care era acum șeful unui program de afiliere a farmaciilor aflat în concurență directă cu firma Rx-Promotion, a lui Vrublevski. Acesta din urmă era convins (și, cred eu, pe bună dreptate) că Gusev sau unul dintre locotenenții lui erau responsabili de scurgerea e-mailurilor interne și a altor documente incriminatoare de la ChronoPay.

Cam în aceeași perioadă în care a fost sustras primul lot de *kompromat* de la ChronoPay, Adam Drake – o sursă din comunitatea antispam căreia îi destăinuisem unele dintre apelurile telefonice ciudate ale lui Vrublevski – mi-a scris prin e-mail despre un mesaj bizar pe care tocmai îl primise. Corespondentul lui misterios, care folosea pseudonimul „Despduck", spunea că a avut acces la baza de date a programelor GlavMed și SpamIt, care generau un procentaj uriaș din spamul mondial. „Desp", din pseudonimul folosit de el, avea la bază porecla aleasă de Igor „Desp" Gusev, cel care fondase ChronoPay cu Vrublevski în 2003, iar după doi ani a creat singur SpamIt și GlavMed.

Drake scria următoarele:

> Brian,
>
> Ai postat recent un text despre o anchetă a guvernului rus cu privire la operațiile firmei SpamIt („Following the Money, Part II" – krebsonsecurity.com/2010/05/following-the-money-part-ii/).
>
> Un tip din Rusia m-a contactat, pretinzând că este prieten cu un fost membru al grupului SpamIt–GlavMed. Are multe informații pe care vreau să ți le transmit pe căi confidențiale. Spun asta pentru că voiam să-ți știu părerea, iar el susține că ți-au fost oferite și ție unele informații despre povestea respectivă și vreau să știu părerea ta despre ele.
>
> El mai susține că are multe date brute referitoare la unele dintre locurile lor de întâlnire, pe care – dacă par reale – le voi preda autorităților. Încă de anul trecut, colaborez cu o echipă specială, din care fac parte membri ai Interpol și FBI și care anchetează grupul respectiv, așa că n-am reușit să fac publice prea multe informații.
>
> Dacă ceva din toate astea nu intră în sfera ta de preocupări, anunță-mă, deși cred că te vor interesa. Același grup se află probabil și în spatele erupției recente de „antiviruși" falși.
>
> Altfel, sper că o duci bine.

Am recunoscut imediat mâna lui Vrublevski în acest șiretlic și i-am cerut lui Drake să-mi transmită o copie a e-mailului de

la Despduck. Nu mi-a venit să-mi cred ochilor când am citit mesajul – se părea că cineva transcrisese cuvintele lui Vrublevski în timp ce îl fermeca pe cel care-l asculta cu una dintre poveștile lui incoerente, dar relatate cu entuziasm. Scrisoarea conținea peste 2 000 de cuvinte și abunda în teorii complicate despre cei aflați în spatele atacurilor îndreptate împotriva ChronoPay, o companie despre care Despduck vorbea realmente cu mândrie.

I-am spus lui Drake despre bănuiala mea că și el era urmărit de Vrublevski și mi-a mărturisit că un prieten din poliție, care era destul de familiarizat cu Vrublevski și văzuse de asemenea e-mailurile de la Despduck, ajunsese în mod independent la aceeași concluzie.

Scrisorile lui Despduck mai aveau un lucru pe care nu-l puteam defini. O săptămână mai târziu, m-am uitat la corespondența mea anterioară cu Vrublevski și am comparat-o cu e-mailurile de la „Despduck" pe care le primea sursa mea antispam. Un element comun mi-a sărit imediat în ochi. Atât Despduck, cât și Vrublevski scriau cu majusculă cuvintele „Tine", „Tu" sau „Te", indiferent de poziția lor în frază sau de câte ori erau folosite. Acest lucru nu se observa la niciun alt cuvânt din e-mailuri care nu trebuia scris cu majusculă.

Apoi, mi-am amintit de e-mailul amenințător, cel cu „ochișorii", pe care-l primisem imediat după ce l-am sunat pe Vrublevski pentru a-i cere un comentariu despre afirmațiile lui Ponomarev. Acolo întâlnisem acel fel de a scrie. Lucrurile începeau să se lege.

Dar de ce s-ar fi străduit Vrublevski într-atât să mă câștige de partea lui și, în același timp, să mă constrângă să cooperez cu el? Sursa mea antispam mi-a oferit răspunsul, trimițându-mi câteva e-mailuri primite de la Despduck. Conform acestora, Vrublevski credea că acceptasem bani de la rivalul lui, Gusev, în schimbul publicării unor articole despre acțiunile sale. Vrublevski părea, de asemenea, convins că eram mână în mână cu personaje dubioase aflate în spatele Russian Business

Network (RBN), despre care am vorbit pe larg în prima jumătate a capitolului 2.*

Despduck scria (tot cu T în „Tu"):

1. Poți să mă crezi sau nu, dar Brian Krebs a fost de fapt plătit de RBN (adesea, prin intermediul GlavMed) pentru a-și face publice cercetările. Toate informațiile lui se bazează în realitate pe faptul că re-partners.biz are adresa sediului ChronoPay, ceea ce, desigur, este o porcărie. Oricine poate pune orice adresă oriunde.
2. Apoi, Ilia Ponomarev (care NU este un politician rus de frunte) le-a scris polițiștilor ruși, încercând să i-o tragă cumva lui Vrublevski pe baza informațiilor lui Krebs. O încercare stupidă, probabil că a făcut-o doar ca să pară că se pot obține mai mulți bani de la Desp. Evident, nu s-a întâmplat nimic, deoarece ChronoPay are în Rusia o imagine și un brand foarte puternice. În curând, ChronoPay îl va da în judecată pe Krebs, iar Ponomarev și-a schimbat deja opinia și a trimis altă scrisoare poliției, explicând că nu-l viza pe Vrublevski.
3. Toate astea s-au întâmplat pentru că Vrublevski se ocupă din partea guvernului de combaterea spamului și, mai important, de apărarea imaginii Rusiei în străinătate. Spammerii îl urăsc pentru asta. Voi explica mai multe când vei avea întrebări.





Despduck a vorbit încă o dată într-un mod elogios despre Vrublevski, un luptător împotriva criminalității informatice acuzat pe nedrept de mass-media și de rivalii săi de afaceri că ar fi organizat activitatea infamă împotriva căreia pretindea că luptă. Acum eram mai sigur ca oricând că Despduck era Vrublevski.

Pe 12 iulie 2010, o sursă anonimă cu care corespondasem prin e-mail mi-a trimis o altă colecție valoroasă de *kompromat*

* În timp ce Vrublevski se purta ca și cum nu avea nimic de-a face cu RBN, siteurile de spam farmaceutic și programele de distribuire a unor antiviruși falși pe care le gestiona acesta profitau din plin de găzduirea oferită de RBN.

furat de la ChronoPay. Sursa, care a folosit doar numele „Boris" în e-mailurile dintre noi, a spus că îmi transmitea acele date fiindcă se simțea frustrată de autoritățile rusești, acestea părând să considere că Vrublevski nu merita să fie luat la rost pentru mită, cu atât mai puțin să fie cercetat.

> Brian,
>
> Acest fișier conține informații *complete* despre activitatea infracțională a firmei ChronoPay și a lui Pavel Vrublevski personal, cu privire la legalizarea banilor ilegali [sic]. Noi am încercat toate metodele disponibile în Rusia, dar poliția coruptă frânează [sic] aducerea cazului respectiv înaintea instanței și tărăgănează lucrurile. Sperăm că vei putea utiliza eficient aceste informații în lupta pentru un internet curat. Același fișier a fost transmis FBI acum două săptămâni.
>
> Mult noroc,
>
> Boris

E-mailurile de la ChronoPay divulgate de Boris – colecția valoroasă de documente la care am făcut referire la sfârșitul capitolului 2 – arată că Vrublevski l-a angajat pe hackerul Nooder Tovreance pentru a sparge serverul SpamIt și a fura informații cu privire la plățile și clienții companiei. Într-un schimb de mesaje între cei doi, care a început la 8 aprilie 2010 și s-a terminat la începutul lunii iunie, Tovreance s-a oferit să-i vândă lui Vrublevski baza de date pentru 20 000 de dolari, dar a spus că trebuia să împartă fișierele ce aveau să fie transferate în mai multe loturi din cauza dimensiunii bazei de date.

Cei doi au bătut în cele din urmă palma pentru 15 000 de dolari, care urmau să fie plătiți în WebMoney, o monedă virtuală populară în Rusia și Europa de Est. Prima plată, de 7 500 de dolari, trebuia să fie efectuată într-un portofel WebMoney specificat de Tovreance în schimbul a jumătate din fișiere, suma rămasă urmând să fie plătită după primirea de către Vrublevski a întregii baze de date. Următoarele e-mailuri arată că Vrublevski a plătit prima tranșă de 7 500 de dolari, dar nu și pe a doua, după primirea bazei de date

promise. Când am discutat cu el, Tovreance a confirmat că Vrublevski îl angajase ca să-i facă rost de datele de la GlavMed și SpamIt și că, într-adevăr, Vrublevski nu-i plătise decât jumătate din suma promisă.

La aproximativ o săptămână după scurgerea *kompromatului* de la ChronoPay, Drake a telefonat ca să-mi spună că Despduck îi trimisese o copie a bazei de date SpamIt și GlavMed. În acel moment, începusem să cred că, așa cum Vrublevski se ascunsese după numele „Despduck" în sustragerea bazei de date cu clienții GlavMed–SpamIt, Gusev folosea identitatea „Boris" pentru a mă alimenta cu informații furate de la ChronoPay.

Baza de date GlavMed–SpamIt mi-a parvenit a doua zi după ce am publicat pe blog informația cu privire la un nou vierme informatic, extrem de complex, care părea să fi fost realizat pentru spionaj. Postarea mea a fost primul articol destinat publicului larg despre un malware de o complexitate fără precedent, care avea să devină cunoscut sub numele de „Stuxnet" – un vierme despre care specialiștii au descoperit mai târziu că era o armă informatică concepută de serviciile secrete israeliene și americane, într-o încercare încununată de succes de a întârzia punerea în aplicare a planurilor nucleare ale autorităților iraniene.

Am postat însă informația despre Stuxnet tocmai când plecam într-o vacanță de o săptămână cu soția și mama mea la York, în statul Maine, și promisesem să nu mai muncesc în perioada aceea. Pe de altă parte, dacă, pentru a continua să scriu despre Stuxnet, ar fi trebuit să vorbesc cu zeci de persoane la telefon, cercetarea documentelor primite de la sursa mea antispam putea fi făcută fără ca familia să știe că mă întorsesem la treabă.

Drake mi-a creat un cont pe serverul lui de web și pusese acolo copia arhivei SpamIt. Fișierul conținea aproape 10 GB de date. (Pentru a înțelege mai exact ce înseamnă asta, dacă

baza de date SpamIt ar fi fost transcrisă în cărți cu lățimea de 7,5 cm, ar fi fost necesar un raft de lungimea unui teren de fotbal pentru a le așeza pe toate.)

Eram deja copleșit de mulțimea materialelor interesante de la ChronoPay și a trebuit să șterg date de pe calculatorul meu pentru a copia arhiva SpamIt. Când m-am instalat pe terasa casei de vacanță din Maine, cu laptopul pe genunchi, având ca fundal sonor vuietul oceanului, am început să înțeleg ce muncă uriașă mă aștepta. Trebuia să interpretez informații brute provenite de la doi dintre cei mai mari sponsori ai spamului de pe planetă, lucru care putea atrage mânia celor mai puternici și mai răzbunători infractori informatici.

# Capitolul 4

# SĂ-I CUNOAȘTEM PE CUMPĂRĂTORI

Deși obiectivul meu final era acela de a-i demasca pe botmasterii plătiți pentru a trimite majoritatea e-mailurilor nesolicitate din lume, știam că examinarea datelor care soseau de la cele două programe farmaceutice concurente va dura luni, poate chiar ani de zile. Deocamdată, descoperisem, ici, colo, doar infracțiuni mărunte, așa că, pentru a porni un proces solid împotriva acestor indivizi și pentru a dezvălui activitățile lor rău intenționate, ar fi fost nevoie de cercetări și investigații aprofundate. Am hotărât să dau cât mai repede de persoanele afectate direct de răufăcătorii cibernetici – clienții care cumpăraseră și luaseră medicamente promovate prin spam.

La un moment dat, aproape toți am primit spam despre medicamente sau spam farmaceutic – acele e-mailuri care apar în folderele de mesaje recepționate, în filtrele de spam și în folderele de mail nesolicitat și prin care ni se oferă medicamente ieftine, eliberate pe bază de rețetă sau destinate măririi anumitor părți al corpului. Poate că nu e tocmai șocant faptul că aproximativ 70% din totalul tranzacțiilor efectuate prin intermediul siteurilor farmaceutice ilicite promovate de SpamIt, al lui Gusev, și de Rx-Promotion, al lui Vrublevski, au avut drept obiect medicamente pentru impotență ca Viagra și Cialis. Chiar și clienții GlavMed care nu comandau medicamente pentru tratarea disfuncției erectile (DE) primeau de

obicei asemenea pastile. Aceste farmacii erau atât de încrezătoare în eficiența strategiei lor în cazul DE, încât includeau în mod obișnuit două–patru mostre gratuite în fiecare comandă a clientului.*

Acelora dintre noi care nu s-au gândit niciodată să comande produse de la o farmacie necunoscută, acest lucru li se poate părea riscant și inutil. De ce n-am folosi pur și simplu o farmacie obișnuită? Într-adevăr, am fost extrem de curios să aflu ce i-a determinat pe oameni să se implice în această activitate aparent riscantă și dacă au fost mulțumiți de experiența avută sau dacă s-au simțit păcăliți. M-am gândit că, dacă discutam cu destui cumpărători și constatam că, pe ansamblu, ei nu obținuseră ceea ce așteptau, dezvăluirea acestui lucru putea ajuta la reducerea cererii și, în cele din urmă, la dispariția spammerilor.



Datorită scurgerilor de date de la firmele Rx-Promotion și GlavMed–SpamIt, aveam numele, numerele de telefon, adresele și seriile cardurilor de credit a peste un milion de cumpărători de medicamente promovate prin spam. Unele dintre comenzi erau destul de recente, așa că doream să discut cu acei cumpărători care mai aveau pastile și mi le puteau trimite pentru a fi analizate de un laborator autorizat, ca să vedem ce anume primiseră de fapt.



Am evitat în mod intenționat să-i sun pe cei care au căutat și au plătit pentru imitații de Viagra și Cialis, considerând că persoanele care cumpăraseră medicamente pentru boli și probleme mai grave de la aceste farmacii iresponsabile aveau de relatat cazuri mai interesante și mai înduioșătoare, care m-ar fi ajutat să ajung la esența problemei: cine cumpăra medicamentele acestea și de ce? Ar fi totuși incorect din

* Deși e-mailurile scurse de la ChronoPay arată altceva, Vrublevski neagă din nou că ar fi coproprietar la Rx-Promotion, dar admite că ChronoPay a efectuat plăți pentru programul farmaceutic. Gusev a negat public că ar administra SpamIt, dar dovezile sugerează iarăși altceva.

partea mea să spun că reportajul meu n-a fost influențat și de experiența pe care am avut-o cu una dintre primele persoane cu care am discutat.

La numai câteva zile după ce am început să telefonez unor persoane care cumpăraseră medicamente de la GlavMed, am format numărul unui bărbat care comandase Viagra. Mi-a răspuns nevasta lui, care a izbucnit în plâns când i-am explicat că soțul ei cumpărase un medicament generic din categoria Cialis cu câteva luni în urmă. Nu știuse asta și mi-a spus că nu știa de ce a făcut așa ceva. După acea discuție, din fericire scurtă, am decis să nu mai telefonez clienților care cumpăraseră exclusiv medicamente pentru disfuncția erectilă.

Pe durata a două luni, am sunat peste patru sute de persoane care cumpăraseră medicamente de la SpamIt. Majoritatea fie mi-au închis, fie au refuzat să discute cu mine. Am reușit totuși să vorbesc cu 45 de cumpărători care comandaseră de toate, de la medicamente pentru inimă la antidepresive și pastile pentru tratarea afecțiunilor tiroidei. Am început să-mi formez o imagine mai clară despre cine erau persoanele respective, care erau motivațiile lor și în ce fel acțiunile lor ne afectează pe toți, chiar și pe aceia dintre noi care nu deschid e-mailuri nesolicitate, necum să cumpere ceva promovat de ele.

Mulți – în special activiștii antispam – au o părere proastă despre cei care cumpără articole promovate în acest fel. La urma urmelor, spun ei, dacă nimeni n-ar mai cumpăra de pe siteurile cărora li se face publicitate prin spamul ce ne umple zilnic conturile de e-mail, atunci amploarea industriei spamului și multe dintre riscurile pe care ea le prezintă pentru identitatea și securitatea noastră ar fi probabil mult diminuate. Dar, contrar părerii populare, majoritatea celor care cumpără din spam nu sunt idioți sau nebuni, ci par a fi oameni cu o educație tehnologică precară, care fac alegeri raționale (chiar dacă potențial riscante), bazate pe una sau mai multe motivații primare:

• **Preţul şi accesibilitatea.** Cei care au cumpărat medicamente, în afară de pastile pentru îmbunătăţirea performanţelor masculine, au declarat aproape în unanimitate că au răspuns la spam fie pentru că nu aveau asigurare medicală, fie pentru că aceleaşi medicamente disponibile la farmaciile obişnuite costau de *două până la cinci ori* mai mult decât cele oferite prin intermediul acestor siteuri farmaceutice canadiene aparent legale. (În realitate, spammerii profitau pur şi simplu de buna reputaţie a farmaciilor canadiene legitime. După cum vom vedea în capitolul 5, medicamentele oferite de toate programele farmaceutice de pe internet erau produse mai ales în India şi China, iar siteurile care le vindeau erau cel mai des găzduite de PC-uri controlate de boţi, care fuseseră sparte de spammeri pentru a fi utilizate în expedierea de e-mailuri nesolicitate.)

• **Confidenţialitatea.** Cumpărătorul doreşte să achiziţioneze anumite medicamente în mod discret, fie pentru că-i este ruşine sau este timid, fie pentru că se simte obligat să ascundă ceva de o soţie sau iubită. În această privinţă, majoritatea clienţilor cu care am discutat se împărţeau în două tabere: cei care se tratau singuri de boli venerice şi cei care comandau medicamente împotriva impotenţei. Din păcate, istoricul comenzilor indică faptul că unii dintre aceşti cumpărători se încadrează în ambele categorii.

• **Comoditatea.** Solicitarea unor medicamente fără reţetă şi livrarea lor acasă reprezintă o metodă extrem de convenabilă. În plus, mulţi dintre cei cu care am vorbit mi-au spus că ei cumpărau pur şi simplu medicamente ce le fuseseră prescrise anterior pentru o afecţiune similară sau asociată. Practic, se tratau singuri şi nu considerau că trebuie să plătească pentru o vizită la medic sau să accepte preţurile mai ridicate percepute de farmaciile locale.

• **Recreerea sau dependenţa.** Cumpărătorii din această categorie au achiziţionat în special medicamente a căror utilizare

și vânzare fuseseră restricționate în SUA, de obicei pentru că puteau crea dependență. Era vorba în primul rând despre analgezice ca oxicodona, hidrocodona și tramadolul, medicamente pentru slăbit ca fentermina (un stimulent puternic) și somnifere ca Soma și Lunesta. Poate datorită dependenței create de unele dintre ele, clienții din această categorie tindeau să fie cei mai loiali și mai profitabili.

## PREȚUL

Clienții SpamIt cumpărau medicamente din diverse motive, dar principalul considerent pe care l-am auzit a fost accesibilitatea – în special de la cei care au cumpărat medicamente pentru tratarea afecțiunilor cronice.

Nu este întâmplător faptul că majoritatea clienților SpamIt sunt din SUA, țara cu cele mai mari prețuri din lume la medicamentele eliberate pe bază de rețetă. În SUA, prețurile la medicamente sunt mult mai mari decât în Canada, India, Marea Britanie și multe alte țări, în mare parte fiindcă acestea au impus restricții în privința prețurilor. În 2012, prețul medicamentelor generice din SUA a crescut în medie cu 5,3%, în timp ce costul medicamentelor originale a crescut cu peste 25%, potrivit unui studiu realizat de Health Care Cost Institute.

Alți factori care au crescut costul medicamentelor eliberate pe bază de rețetă au fost: creșterea cererii pentru aceste medicamente în ultimul deceniu, promovarea intensă a medicamentelor originale, cu prețuri mai ridicate, îndreptată spre consumatori și medici, încercările producătorilor de medicamente de a recupera costurile substanțiale ale cercetării și dezvoltării și costisitorul joc de noroc care este procesul de lansare a unui medicament nou pe piața SUA. (Conform unui articol publicat în 2012 în revista *Forbes*, costurile suportate de o companie farmaceutică pentru a plasa un medicament nou pe piață ajunge în prezent la 350 de milioane de dolari.)

Interesant este faptul că zeci de clienți ai SpamIt cu care am discutat au declarat că pastilele primite nu puteau fi deosebite de aceleași medicamente pe care le achiziționaseră din farmaciile locale, cu excepția faptului că cele comandate on-line au costat mult mai puțin. De fapt, mulți clienți au fost atât de satisfăcuți, încât au revenit la același site și în lunile următoare.

Henry Webb, un agent imobiliar de 42 de ani din California, cumpăra de aproape trei ani de la farmaciile on-line, deși a spus că, înainte de a-l contacta eu, nu știa de fapt de la cine cumpăra. Webb se luptase cu depresia până în urmă cu aproximativ zece ani, când medicul i-a prescris antidepresivul Lexapro. Ani de zile, Webb a plătit aproape 500 de dolari la fiecare nouăzeci de zile pentru a primi acel medicament.

Apoi, într-o zi, a deschis un e-mail nesolicitat care făcea reclamă la Lexapro pentru aproape un sfert din prețul respectiv. De atunci, Webb a comandat de pe mai multe siteuri „de farmacii canadiene", declarând că, deocamdată, nu a avut experiențe negative.

„Pastilele arată exact ca acelea pentru care plăteam 500 de dolari la farmacie – sunt în aceeași cutie și așa mai departe, a spus Webb. Vreau să spun doar că e trist că trăim în această țară și trebuie să căutăm în afara ei medicamente accesibile."

Contactat la câteva luni după discuția inițială, Webb a spus că a renunțat la comenzile on-line după ce a avut experiențe neplăcute cu unele medicamente care-i făcuseră rău. El a avut de asemenea parte de ceva ce-i va afecta la un moment dat pe aproape toți cei care achiziționează produse promovate prin spam: apeluri repetate de la angajați agresivi ai farmaciilor on-line, care au încercat să-l convingă să mai comande produsul respectiv sau să-i vândă alte medicamente.

„Nu mă lăsau în pace și sunau de mai multe ori pe zi, a spus Webb. Nu-mi pot schimba numărul, deoarece este al firmei mele, dar indivizii ăștia sunt foarte șmecheri, schimbând

numărul de la care sună, așa încât am impresia că dau telefon din zona mea. De aceea răspund, pentru că trebuie să fiu la dispoziția clienților mei tot timpul."

Problema prețurilor este agravată de practica puțin cunoscută, dar răspândită în rândul marilor producători farmaceutici, de a plăti rivalilor care produc medicamente generice pentru a amâna cât mai mult introducerea de medicamente cu prețuri mai mici. Potrivit Comisiei Federale pentru Comerț, în anul fiscal 2010, companiile farmaceutice au încheiat un număr nemaiîntâlnit de asemenea acorduri frauduloase. Comisia a constatat că numărul acestor tranzacții a crescut cu peste 60%, de la 19, în anul fiscal 2009, la 31, în anul fiscal 2010. În ansamblu, acordurile realizate în anul fiscal 2010 au vizat 22 de produse farmaceutice de branduri diferite, cu vânzări anuale combinate în SUA de aproximativ 9,3 miliarde de dolari.

Craig S., agent de asigurări de viață din Carolina de Nord, actualmente pensionar, știe din proprie experiență cum este când un producător de medicamente sau o companie de asigurări de sănătate încetează brusc să mai ofere produse generice. Craig a spus că angajatorul său, la care lucra de 20 de ani, îi oferise inițial un plan generos de asistență medicală. Apoi, cu un an înainte de discuția noastră, angajatorul a renunțat la compania de asigurări de sănătate și i-a obligat pe toți angajații să-și deschidă conturi de economii de sănătate („health-care savings accounts", HSA), în care acesta vărsa doar o mie de dolari anual. Medicul lui Craig îi prescrisese multă vreme medicamentul original Actos pentru diabetul de tip 2, iar Craig cumpărase versiunea generică.

În scurt timp însă, a descoperit că versiunea generică a lui Actos nu era oferită prin programul HSA. Cu toate acestea a reușit să utilizeze cardul de credit HSA pentru a se aproviziona cu medicamente pentru 90 de zile de la GlavMed cu 178 de dolari, preț care includea transportul.

„Medicamentul pe care medicul meu vrea să-l iau costă 212 dolari lunar și i-am spus că nu se poate, a zis Craig. În

prezent, mă costă aproximativ o treime din cât m-ar fi costat dacă aș fi cumpărat versiunea originală în fiecare lună prin planul meu de asistență medicală."

Când l-am întrebat dacă-l preocupă calitatea, eficacitatea și siguranța medicamentelor pe care le cumpără de la spammeri, Craig a spus: „Nu prea." El continua să meargă la medic din trei în trei luni, iar medicamentele pe care le comanda la GlavMed păreau să-i țină diabetul sub control.

Principala lui preocupare este aceea că, într-o bună zi, pastilele comandate s-ar putea să nu mai sosească; de altfel, i s-a întâmplat o dată ca o comandă să întârzie o săptămână. Deocamdată însă, furnizorii lui de medicamente de pe internet par să fie foarte atenți. Craig a spus că, la fiecare câteva luni, când mai sunt aproximativ trei săptămâni până la terminarea medicamentelor, începe să primească apeluri telefonice de la persoane cu accent indian, care-l întreabă dacă este pregătit să facă o nouă comandă.



„Steve", din Illinois, își suspecta prietena că-l înșela, dar n-a acceptat pe deplin realitatea până în ziua când a primit o știre zguduitoare prin SMS.

„Aveam nevoie de medicamente din cauză că sufeream de sindromul prietenei infidele, a explicat el jenat, în discuția noastră, despre motivele pentru care a cumpărat de pe internet. Într-o zi, m-a anunțat prin SMS că avea gonoree și că ar trebui să-mi fac și eu analize."

Fusese o lună grea pentru Steve. Nu numai că prietena lui se culcase cu un coleg de serviciu, îl abandonase pe el și-i făcuse cadou o boală venerică (din fericire, tratabilă), dar angajatorul lui – o firmă de analize de mediu – tocmai îl concediase, iar el nu avea asigurare de sănătate.

„Aș fi putut avea o asigurare COBRA, dar asta costă 300–400 de dolari pe lună, a explicat Steve. Iar când n-ai un venit constant și, în plus, trebuie să plătești chirie, rată la mașină și toate celelalte, nu-ți permiți așa ceva."

Fosta lui prietenă i-a trimis grijulie un SMS cu numele medicamentului pe care i-l prescrisese medicul ei: eritromicină sub formă de comprimate de 500 mg. Așa că Steve a intrat on-line, a căutat medicamentul și a găsit exact ce avea nevoie pe un site care pretindea că vinde din Canada. (Siteul de pe care a cumpărat Steve era de fapt găzduit în China prin GlavMed, iar medicamentele erau expediate din India.) Peste șapte zile, după ce a achitat 60 de dolari, Steve a primit antibioticele și a scăpat de boala venerică.

În ciuda circumstanțelor care l-au determinat să cumpere, Steve a spus că experiența generală cu GlavMed a fost pozitivă și că ar cumpăra din nou de la ei dacă ar mai apărea vreo urgență.

„Dacă aș mai face asta? Sigur că da. De ce să plătesc o asigurare medicală și 75 de dolari pentru o rețetă când pot obține medicamentul on-line, cu mai puțin deranj? Vreau să spun că aș fi putut trata cinci persoane cu [numărul de pastile] pe care mi le-au trimis. Deci, în privința prețului, oferta lor este imbatabilă."

Poveștile acestor cumpărători demonstrează că mulți americani apelează la medicamente promovate prin spam deoarece alternativa este de câteva ori mai scumpă sau pentru că asigurarea nu acoperă medicamentele ce le-au fost prescrise. În timp ce experiența pozitivă a lui Steve, care a comandat pastile pentru o singură utilizare, pare a fi destul de des întâlnită, cei care achiziționează în mod repetat medicamente pentru tratarea unor afecțiuni cronice au mai multe șanse ca, mai devreme sau mai târziu, să primească produse cu probleme.

Așa cum vom vedea în capitolul 5, aceasta se datorează faptului că farmaciile care-și fac publicitate prin spam tind să cumpere medicamente ieftine de la zeci de surse din toată lumea, dintre care unele par să nu aibă nicio responsabilitate în ceea ce privește siguranța și eficacitatea produselor lor. Medicamentele de calitate inferioară le pot face rău clienților, ca în cazul lui Henry. În cazuri extreme, după cum vom vedea în capitolul 5, cele care nu corespund standardelor îi pot trimite la spital sau, mai rău, la morgă.

Avocat de profesie, „John", din Washington, DC, petrecea foarte mult timp la birou și căuta o cale rapidă și ușoară de a-și dezvolta mușchii. După ce a studiat mai multe forumuri de culturism on-line, a început să cumpere steroizi îndoielnici de pe un site recomandat de oameni versați în acest domeniu. După câteva luni și un regim scurt de antrenamente fizice, pastilele l-au ajutat să-și mărească masa musculară cu câteva kilograme.

În februarie 2010 însă, mameloanele lui John s-au umflat și au devenit sensibile. Îngrijorat să nu fie un efect secundar al steroizilor (și nedorind să-i spună medicului său despre regimul cu steroizi), a revenit pe forumurile pentru culturiști pentru a cere sfatul tovarășilor săi.

Aceștia i-au spus că suferă de ginecomastie determinată de consumul steroizilor, adică dezvoltarea unor glande mamare anormal de mari la bărbați, ceea ce duce la creșterea sânilor.



„Majoritatea celor de pe forumuri numesc această afecțiune «mamele de curvă» (*bitch tits*), a spus John. Băieții mi-au spus că, dacă nu se rezolvă cu medicamente, ai nevoie de o intervenție chirurgicală pentru a-ți repara pieptul și n-am vrut să fac așa ceva."

Soluția în cazul lui John – potrivit noilor lui prieteni – presupunea administrarea altor medicamente menite să contracareze acțiunea hormonilor care cauzează afecțiunea respectivă. Printre ele se număra „Femara", un medicament prescris adesea pacientelor cu cancer mamar în fază timpurie, aflate în postmenopauză.

John a căutat pe web și a ajuns să cumpere, cu 136 de dolari, pastile Femara de 2,5 mg, pentru două săptămâni, de pe un site din rețeaua GlavMed numit elitepharmacy.com. A așteptat trei săptămâni, dar medicamentele n-au mai sosit, așa că a anulat comanda și a comandat de la altă farmacie on-line care nu era afiliată rețelei GlavMed. (John își amintește că cele două siteuri arătau aproape la fel.) Siteul la care comandase

întâi şi-a cerut scuze pentru întârziere şi i-a returnat suma pe care o plătise cu cardul de credit.

Medicamentele pe care le-a primit de la al doilea site au sosit într-un plic expediat din India, dar medicamentele în sine erau ambalate în blistere cu numele brandului Novartis tipărit impecabil de mai multe ori pe folia de staniol de deasupra pastilelor.

John spune că medicamentele arătau la fel cu cele originale şi au redus sensibilitatea şi inflamaţia mameloanelor, ducând efectiv la dispariţia problemei sale.

„La început, am fost cam circumspect, dar a mers, a spus John. De asemenea, am crezut că pierd timpul anulându-mi comanda. Cumva mi-am dat seama că era o afacere necurată... dar mi-au dat banii înapoi."

Experienţa lui John arată până unde pot merge programele farmaceutice ilicite pentru a asigura satisfacţia clienţilor. Scopul lor nu este neapărat să nu-l supere pe client. Mai degrabă, cei care administrează aceste afaceri vor face aproape orice pentru a-i împiedica pe clienţi să iniţieze „restituirea sumei plătite", proces în care clientul îşi cere banii înapoi, invocând o fraudă sau o altă neregulă săvârşită de un magazin on-line. Comercianţii care primesc prea multe cereri de restituire plătesc taxe de procesare mult mai mari şi pot fi în cele din urmă amendaţi ori li se pot închide conturile.

Baza de date despre clienţii GlavMed arată că programul respectiv avea un personal de asistenţă format din zeci de persoane, care operau non-stop, telefonic şi prin chat on-line, răspunzând la nemulţumirile clienţilor sau la întrebările despre comenzile plasate.

Vişnevski, spammerul amintit în capitolul 1, care a colaborat cu GlavMed–SpamIt la finanţarea creării botnetului Cutwail, a declarat, într-o discuţie avută prin mesageria instantanee, că persoanele care cumpără de pe siteurile farmaceutice îşi pot recăpăta întotdeauna banii, telefonând şi înregistrând o reclamaţie la un număr de telefon special.

„Banca îl va penaliza pe orice comerciant cu cereri de restituire care depăşesc 1% din totalul vânzărilor", a spus el. „De aceea, nimeni nu va risca să piardă [contul de procesare a cardurilor] din cauza nereturnării banilor, iar toţi cei care cer [departamentului de asistenţă pentru clienţi al programului de farmacii afiliate] să li se restituie banii şi-i primesc."

## AUTOMEDICAŢIA

Kimberly din Virginia a cumpărat de la GlavMed fără a avea o recomandare de la medic, dar a primit banii înapoi după ce s-a plâns că n-a fost mulţumită de ceea ce cumpărase. Ea şi soţul ei aveau probleme în conceperea unui copil. Bărbatul, care era militar, pleca adesea în misiuni lungi şi ea dorise să rămână însărcinată înainte ca soţul să plece pentru încă un an în străinătate. Kimberly, care era asistentă medicală, a spus că hotărâse să comande on-line medicamentul pentru fertilitate Clomid, deoarece ştia că asta ar fi prescris un medic specialist în infertilitate.

„În principiu, ştiam cum să-l folosesc şi ce trebuia să fac, iar în loc să-i plătesc unui doctor o căruţă de bani pentru a-mi explica ceea ce ştiam deja, am ales s-o fac singură, povestea Kimberly. N-am comandat de la primul site pe care l-am găsit. Am mai căutat şi am văzut că mai multe siteuri făceau trimitere la un anumit site."

Câteva săptămâni mai târziu, un plic maro a sosit prin poştă, cu ştampile din India. Pilulele Clomid erau ambalate în obişnuitul blister, dar Kimberly a observat că data de expirare ştanţată era deja depăşită. A cerut să i se restituie banii şi i-a primit fără întârziere. Ironia a făcut să descopere că este însărcinată la doar câteva zile după ce a primit banii înapoi – medicamentele nu mai erau necesare.

Contul de e-mail i-a fost însă bombardat cu spam după ce a comandat medicamentele on-line, iar Kimberly îşi face mai

departe griji că farmacia on-line poate să-i retragă fraudulos bani de pe cardul de credit.

„De atunci, a spus ea, mi-au trimis un milion de mesaje. Știu că n-a fost ideea cea mai bună să comand medicamentele on-line, dar în momentul respectiv eram disperată. Mă bucur foarte mult că n-am luat medicamentul. Probabil că ar fi făcut rău fătului pe care-l aveam deja în burtă."

Vișnevski a confirmat că oamenii sunt adesea bombardați cu spam după ce fac o comandă sau răspund la oferte nesolicitate primite prin e-mail. Asta pentru că adresele cumpărătorilor cunoscuți sunt o marfă valoroasă, care se revinde adeseori sau pur și simplu este furată de alți hackeri și spammeri. (Amintiți-vă că lista lui Vișnevski, care conținea două miliarde de adrese de e-mail, a fost lăsată pe serverele lui McColo. Ea putea fi descărcată de oricine se întâmpla să descopere linkul necesar pentru accesarea fișierului.)

Vișnevski spunea însă că este greșit să se creadă că o comandă făcută pe siteurile unor farmacii on-line va duce la fraudarea cardurilor de credit. Niciunul dintre spammerii care lucrează pentru SpamIt, GlavMed sau orice alt program de spam farmaceutic nu le permite farmaciilor afiliate să vadă datele de pe cardul clientului, deoarece vor să păstreze acele informații doar pentru ei.

„Numai administratorii programului farmaceutic le-ar vedea, iar ei nu obțin niciun beneficiu din fraudarea cardului respectiv, deoarece comerciantul ar risca să-și piardă contul de procesare a cardurilor" ca rezultat al creșterii numărului restituirilor și al acuzațiilor de fraudă, a spus el.

## DEPENDENȚA

Majoritatea cumpărătorilor care se încadrau în această categorie au refuzat să discute cu mine. De asemenea, toți comandaseră de pe siteuri ale unor farmacii afiliate care

lucrau pentru Rx-Promotion, firma lui Vrublevski. Aceasta își crease o nișă de piață, fiind unul dintre puținele programe de farmacii afiliate care promovau și vindeau analgezice, stimulente și alte substanțe a căror distribuție este strict controlată de autoritățile din SUA și din alte țări. (Datele arată că GlavMed a oferit, în primii doi ani, și medicamente supuse restricțiilor, dar nu le mai vindea atunci când am început acest proiect.)

În vârstă de 41 de ani, Goran era un fost prizonier de război din Europa de Est, stabilit în SUA. Cu aproape 20 de ani în urmă, s-a lovit rău la spate. Medicii au încetat de mult să-i prescrie hidrocodonă, așa că el cheltuiește lunar între 250 și 500 de dolari cumpărând-o de pe internet împreună cu tramadol, chiar dacă acest lucru este un delict în statul său. Date sustrase de la Rx-Promotion arată că el a cumpărat de câteva ori în anul 2010.



Goran mi-a spus că, până acum, a fost mulțumit de medicamentele cumpărate, care sunt la fel de bune ca și cele prescrise de medicul său pentru a-i scădea durerea. Medicamentele comandate on-line soseau de obicei din Hong Kong și ajungeau în blistere învelite într-o pungă de plastic cu fermoar.

Fără acele analgezice, spunea el, nu ar fi în stare să se ocupe de afacerea sa din domeniul transporturilor. „În țara asta, știi ce pățești dacă nu lucrezi? a întrebat el. Ajungi în stradă."

Poate că Goran ia medicamente împotriva unor dureri de spate reale, dar eu suspectam că mulți alții nu o făceau pentru asta. Interesant este că baza de date GlavMed indică semne clare de abuz în rândul clienților care au comandat substanțe supuse restricțiilor în anii în care rețeaua vindea așa ceva. Am transmis datele despre clienții GlavMed lui Gary Warner, director de cercetare în domeniul criminalității informatice la University of Alabama din Birmingham, care le-a analizat pentru a vedea dacă se puteau determina ușor anumite caracteristici.

„Am descoperit că, dacă ai fost un client GlavMed care a făcut mai mult de cinci comenzi, exista o șansă de 80–85%

să fi cumpărat tramadol sau Soma, a spus Warner. Întrebarea este dacă acei clienți au cumpărat medicamentele pentru uz personal sau pentru a le revinde? Pe stradă, ele valorează aproximativ cinci dolari pastila, ceea ce înseamnă că, dacă comandai un flacon prin GlavMed și le vindeai la bucată, puteai obține un profit de 1 300 de dolari pe flacon."

Cercetătorii de la UCSD cărora le-am pus la dispoziție datele cu privire la vânzările Rx-Promotion au găsit, de asemenea, indicii clare că o sursă importantă a veniturilor obținute de respectiva farmacie o reprezentau clienții fideli. Echipa a constatat că vânzările de analgezice și alte medicamente supuse unor restricții foarte stricte în SUA au produs 48% din totalul veniturilor programului Rx-Promotion.

„Faptul că astfel de medicamente sunt prezente într-o proporție covârșitoare în vânzările Rx-Promotion (iar în cazul unor medicamente ca Soma și tramadol, în vânzările SpamIt) confirmă ipoteza că abuzul poate fi un factor important pentru această componentă a cererii", a scris echipa de la UCSD într-un studiu în care a prezentat concluziile desprinse în urma analizei.

În mare parte, n-am izbutit să aflu direct de la cei cu care am discutat detalii despre eficacitatea și siguranța medicamentelor pe care le-au primit de la GlavMed sau Rx-Promotion. Aproape toți cei cu care am vorbit mi-au promis că o să trimită o pastilă sau două din pachetele primite, însă numai unul a făcut-o. Pachetul conținea atât Viagra contrafăcută, cât și un alt medicament care s-au strivit și s-au amestecat, astfel că n-au putut fi analizate.

Prin urmare, deși aveam câteva informații bune despre motivele pentru care oamenii comandau aceste medicamente și perpetuau astfel problema spamului, am ajuns la concluzia că, pentru a înțelege datele despre clienții și rețelele GlavMed și Rx-Promotion, aveam nevoie de ajutor din partea lui Warner și a altor cercetători importanți, care aveau capacitatea și mijloacele necesare testării acestor medicamente. Atunci nu

ştiam că aceşti cercetători încercaseră să descopere acelaşi lucru pe cont propriu, dar fuseseră blocaţi de birocraţie şi chiar de industria farmaceutică. Urma de asemenea să descopăr consecinţele mult mai întunecate şi mai sinistre ale alegerilor făcute de cumpărătorii de medicamente on-line.

# Capitolul 5

# RULETA RUSEASCĂ

La nici o zi după Crăciunul anului 2006, Marcia Bergeron a murit din cauza otrăvurilor amestecate în câteva medicamente pe care le comandase de la o presupusă farmacie canadiană on-line. Cadavrul a fost descoperit de un vecin și în casa ei au fost găsite peste o sută de pastile generice, printre care un sedativ, un medicament împotriva anxietății și acetaminofen.

Bergeron avea 57 de ani și locuia pe insula Quadra din Columbia Britanică, Canada, iar în zilele dinaintea morții începuse să-i cadă părul și să i se înceţoşeze vederea. Potrivit raportului întocmit de medicul legist, „doamna Bergeron suferise de mai multe simptome. În câteva e-mailuri adresate unei prietene, îi spunea acesteia că are greață, diaree, dureri articulare și alte probleme. Prietenii apropiați știau că îi cădea părul și că avea probleme de vedere. În zilele dinaintea decesului, se simțea foarte obosită și bolnavă".

Autopsia a arătat faptul că Bergeron fusese otrăvită lent cu substanțe chimice foarte periculoase existente în medicamentele despre care Serviciul de Medicină Legală din Columbia Britanică spunea că fuseseră comandate de la o farmacie on-line.

Testele toxicologice au indicat că multe dintre pastilele respective conțineau doze foarte mari de metale grele, care fuseseră folosite probabil ca excipiente sau erau provenite de la o instalație contaminată. Printre substanțele chimice găsite în pilule se numărau uraniul și plumbul, ambele putând fi letale sau foarte dăunătoare chiar și în doze mici.

Nu se știe ce program farmaceutic ilicit de pe internet a susținut siteul de pe care comandase Bergeron. Medicamentele achiziționate de GlavMed și alte parteneriate farmaceutice ilicite sunt comercializate ca și cum ar proveni de la farmacii din Canada, care este renumită în toată lumea pentru prețurile accesibile. Majoritatea medicamentelor de la GlavMed par să fi fost expediate însă de șase–șapte farmacii sau furnizori din India, care se numără în prezent printre cele mai mari surse mondiale de medicamente originale și generice. Restul par a fi provenit de la peste 40 de producători și furnizori din China, India și Pakistan, dintre care unii păreau să revândă medicamente originale la prețuri foarte mici, iar alții nu. Era limpede că farmaciile la care apela Bergeron nu făceau acest lucru.

India deține cunoștințele, forța de muncă și infrastructura necesare fabricării anuale a unor cantități uriașe de medicamente, încurajând înflorirea unei industrii care înregistrează venituri anuale de 10 miliarde de dolari, chiar dacă autoritățile indiene refuză în mod obișnuit să autorizeze multe medicamente fabricate în Occident.

Așa cum scriau Vikas Bajaj și Andrew Pollack în martie 2012 pentru *New York Times*, conflictul dintre India și producătorii occidentali de medicamente în privința brevetelor datează din 1970, când țara a încetat să mai acorde brevete pentru medicamente. A reluat acordarea lor în 2005, ca parte a unui acord cu Organizația Mondială a Comerțului, însă acesta nu s-a aplicat retroactiv pentru medicamente create înainte de 1995.

De atunci, scria *New York Times*, India a devenit un fel de farmacie a lumii, iar în ultimele decenii, a fost cel mai mare furnizor de medicamente generice, ieftine, care au salvat viața multor oameni din țările sărace ale lumii. Producătorii occidentali de medicamente au acuzat că, prin limitarea acordării de brevete în anumite cazuri și încurajarea dezvoltării de

medicamente generice, ieftine, guvernul indian și industria farmaceutică indiană înăbușeau inovarea și reduceau profiturile, care sunt esențiale pentru continuarea cercetării și dezvoltării unor medicamente vitale. Producătorii indieni de medicamente afirmă că practicile lor asigură accesul țărilor mai sărace la medicamente ieftine pentru flageluri ca HIV și cancerul.

Astfel, într-un conflict juridic mult mediatizat, producătorii indieni de medicamente s-au luptat cu gigantul farmaceutic elvețian Novartis pentru ca firmele indiene să poată produce mai departe versiuni generice ale medicamentului Gleevec, care tratează eficient unele tipuri de leucemie. După cum notează *New York Times*, Gleevec poate costa până la 70 000 de dolari pe an, în timp ce versiunile generice indiene se vindeau cu aproximativ 2 500 de dolari pe an. La sfârșitul lunii martie 2013, Curtea Supremă din India a decis că medicamentul Gleevec nu reprezenta o invenție reală.

Problema este că lupta admirabilă, chiar dacă egoistă, a Indiei pentru producerea de medicamente generice accesibile altor oameni nu ține seama și de siguranța și eficacitatea lor. Pe de altă parte, industria farmaceutică din SUA afirmă că medicamentele eliberate pe bază de rețetă care sunt produse în afara așa-numitului „lanț de aprovizionare aprobat" sunt cel puțin contrafăcute, probabil neconforme și chiar periculoase sau letale. Indiferent dacă lucrurile stau sau nu stau mereu așa, producătorii americani de medicamente au dreptate în legătură cu un lucru: majoritatea medicamentelor vândute de farmacii ilicite on-line nu sunt produse în unități reglementate și de aceea prezintă riscuri serioase pentru oricine alege să le folosească.

Statisticile cu privire la industria farmaceutică ilicită – și implicațiile ei asupra sănătății clienților – sunt cu adevărat terifiante. Potrivit Organizației Mondiale a Sănătății, aproximativ 8% dintre ingredientele farmaceutice active importate în SUA sunt contrafăcute, neaprobate sau de calitate

inferioară, iar 10% din comerțul farmaceutic la nivel mondial – adică 21 de miliarde de dolari – implică medicamente contrafăcute. Într-un studiu realizat de International Journal of Clinical Practice (IJCP), publicat în 2012, se afirmă că cifra respectivă ar fi de peste trei ori mai mare. Studiul IJCP estimează că vânzările globale de medicamente contrafăcute s-au dublat între 2005 și 2010, depășind în prezent 75 de miliarde de dolari. Organizația Alliance for Safe On-line Pharmacies estimează că, în orice moment, operează pe piață 30 000–40 000 de vânzători on-line de medicamente, dintre care doar o mică parte sunt recunoscuți din punct de vedere legal.

Gigantul farmaceutic Merck a analizat recent peste 2 500 de farmacii de pe internet și a constatat că peste 80% dintre siteurile respective își vindeau produsele fără a solicita rețetă. Farmacii on-line gestionate de rețele ca Rx-Promotion și GlavMed–SpamIt nu au cerut niciodată clienților să prezinte rețetă, deși farmaciile on-line autorizate care vând americanilor medicamente pe bază de rețetă trebuie, potrivit legii, să le ceară. Mai mult decât atât, Merck a descoperit că aproape 600 de asemenea farmacii vindeau medicamente la prețuri inferioare celui mai mic preț mediu cu ridicata practicat pe orice altă piață, ceea ce indica limpede faptul că medicamentele erau contrafăcute – și, foarte posibil, nesigure.

Mulți care au cumpărat de la farmacii on-line afiliate rețelelor Rx-Promotion și SpamIt și-au exprimat surprinderea spunând că au primit pachete expediate direct din India și China. Potrivit unui raport din 2010 al US Government Accountability Office (GAO), în țările respective se produc marea majoritate a medicamentelor pe care le cumpărăm de la farmacia din cartier. GAO a constatat că aproximativ 80% dintre ingredientele primare ale tuturor produselor farmaceutice – inclusiv cele comercializate de farmaciile on-line ilicite, farmaciile on-line autorizate și chiar lanțuri de farmacii clasice precum CVS și Walgreens – provin de la fabrici indiene și chineze.

Problema nu este că medicamentele respective sunt produse în afara Americii de Nord pentru consumatori din SUA și Canada, ci că nu se știe dacă furnizorii folosiți de rețele ilicite ca SpamIt și Rx-Promotion livrează medicamente originale și generice lanțului de aprovizionare a farmaciilor recunoscute de lege și autorizate în SUA și în străinătate – și, mai important, dacă medicamentele pe care le produc aceștia sunt sau nu sunt sigure.

De exemplu, farmaciile SpamIt s-au bazat pe medicamente vândute în cantitate mare de cel puțin 40 de furnizori diferiți, dar marea majoritate a medicamentelor vândute prin siteurile proprii promovate prin spam proveneau de la șase–șapte furnizori din India și Hong Kong. Potrivit informațiilor obținute din baza de date a SpamIt și din discuțiile avute pe chat de Stupin, printre principalii furnizori ai SpamIt se numărau Sai Balaji Enterprises și Hemant Pharma (care opera sub numele de „Chinmay Overseas"), ambele din Mumbai (India). Alți furnizori importanți erau Trans Atlantic Corp., cu sediul în Hong Kong, și Shri Kethlaji Traders, din Sumerpur (India).

Problema este că sistemul de comenzi al GlavMed–SpamIt pare să fi selectat în mod automat furnizorii și expeditorii bazându-se pe prețul cel mai mic oferit de aceștia în ultima vreme pentru clasa de medicamente căutată de client. Companiile farmaceutice bazate pe spam nu au habar dacă aceste medicamente sunt sigure – sau dacă sunt măcar originale ori contrafăcute, eventual pline cu otrăvuri, cum au fost cele care au ucis-o pe Marcia Bergeron.

Pe scurt, clienții care comandă medicamente din spam s-ar putea să joace o periculoasă ruletă rusească.

Cercetând mai departe, am descoperit că GlavMed a ținut cu scrupulozitate evidența reclamațiilor și diverselor cereri adresate serviciului de asistență pentru clienți. Mii de reclamații ale clienților au apărut în baza de date a GlavMed care mi-a parvenit, dar relativ puține se refereau la calitatea medicamentelor

livrate. Majoritatea lor erau legate de întârzieri în primirea medicamentelor comandate sau erau făcute de clienți care primiseră alte medicamente decât cele comandate ori fuseseră nemulțumiți de felul în care fuseseră ambalate.

O excepție o constituia tranzacția realizată de Deborah G., din Marea Britanie. Deborah a comandat medicamente pentru slăbit și alte articole de pe pillaz.com – un site promovat de un spammer care lucrează pentru programul de afiliere GlavMed. Potrivit bazei de date cu reclamațiile clienților GlavMed, pilulele comandate de Deborah au trimis-o la urgențe. Deborah s-a descris ca fiind o femeie de 43 de ani, care cântărea peste 90 kg, nu avea alergii și nici nu urma un tratament medical în acel moment. În 2010, ea a plătit 437,39 de dolari (fără taxele de transport) pentru mai multe medicamente eliberate pe bază de rețetă, cum ar fi:

- 180 de comprimate (de câte 20 mg) de Acomplia, un medicament antiobezitate;
- 60 de doze de Xenical, un medicament care blochează absorbția grăsimilor din anumite alimente;
- necesarul pe trei luni de Hoodia, un supliment organic pentru slăbit;
- patru tuburi de cremă cu tretinoin împotriva acneei.

La scurt timp după ce a ingerat noile pastile, Deborah a făcut o depresie puternică și a trebuit să fie internată în spital după ce a început să aibă probleme stomacale. Suspectând că tabletele primite în urma comenzii on-line ar putea fi alterate, ea le-a dus la un laborator pentru a fi analizate.

„La analize, au descoperit că erau complet false", a menționat Deborah în reclamația trimisă prin e-mail serviciului de asistență pentru clienți al GlavMed. Analizele au arătat că unele pastile conțineau diverse ingrediente inactive și în mod clar periculoase, printre care otrăvuri, ciment și pudră de talc.

Ulterior, Deborah a depus o reclamație amenințătoare pe siteul de unde comandase.

„Vreau TOȚI banii înapoi. Voi returna cu plăcere tabletele și nu voi mai întreprinde alte acțiuni", a scris ea într-un comentariu inclus în baza de date SpamIt. „Dar dacă nu voi primi banii, nu voi avea altă variantă decât să mă adresez poliției și autorităților vamale care se ocupă de medicamentele contrafăcute și, credeți-mă, vă voi da în judecată. Doresc restituirea imediată a tuturor banilor pe care i-am plătit pentru otrăvurile voastre."

Documentele arată că siteul afiliat SpamIt s-a conformat și a rambursat toți banii în contul cardului de credit al lui Deborah. A reieșit încă o dată că ultimul lucru pe care și-l doresc farmaciile on-line ilicite este să atragă atenția autorităților sau să aibă clienți nemulțumiți, care-și cer banii înapoi, ceea ce ar putea afecta capacitatea farmaciei de a lucra cu carduri de credit (lucru care ar însemna încheierea activității) și ar putea atrage amenzi însemnate.

Având în vedere cantitatea de medicamente contrafăcute care inundă anual piețele din America de Nord și Europa – ca și potențialele pagube produse mărcilor și pierderile financiare provocate de farmaciile ilicite – ați crede că puternica și influenta industrie farmaceutică își folosește puterea pentru a arăta cât de periculoase pot fi aceste medicamente. Într-adevăr, povestea morții lui Bergeron este aproape întotdeauna menționată într-o anumită formă ori de câte ori experții aliați industriei farmaceutice vorbesc despre necesitatea eradicării farmaciilor ilicite de pe internet.

Cu toate acestea, nici Food and Drug Administration (FDA), nici giganții industriei farmaceutice nu par să fi luat măsuri concrete împotriva acestor concurenți, deși ar fi ușor de demonstrat că medicamentele oferite de ei conțin ingrediente dăunătoare sau cel puțin niveluri periculos de scăzute ori de ridicate ale ingredientelor active, comparativ cu versiunile autorizate ale aceloraşi produse.

John Horton, președintele companiei LegitScript, care deține o bază de date cu mii de siteuri farmaceutice autorizate

și „ilicite", spunea că FDA publică ocazional rezultatele analizelor chimice ale unor suplimente dietetice și medicamente eliberate pe bază de rețetă, cumpărate de la farmacii on-line, dar că au fost efectuate puține studii cuprinzătoare.

„Trebuie să spunem că nu prea există analize, a declarat Horton, care a fost consilier al Casei Albe pentru probleme de politică în domeniul medicamentelor în timpul administrației George W. Bush, din 2002 până în 2007. Cred că una dintre probleme este costul acestor analize. De asemenea, este dificil de studiat și analizat științific compoziția chimică a medicamentelor comandate de la farmaciile ilicite deoarece ele își schimbă în mod constant furnizorii."

Potrivit celor de la LegitScript, există peste 41 000 de farmacii active pe internet, însă doar 0,5% dintre ele (cu puțin peste 200) sunt autorizate și funcționează legal. Cu alte cuvinte, dacă veți comanda de la o asemenea farmacie, există peste 99% șanse ca aceasta să fie ilegală, neautorizată. LegitScript consideră farmaciile ca fiind legale dacă îndeplinesc o serie de criterii, printre care înregistrarea la US Drug Enforcement Agency și existența unei licențe de vânzare a medicamentelor. Cel mai important este însă faptul că farmaciile respective trebuie să ceară și să primească o rețetă medicală înainte de a vinde medicamente clienților americani.

Colac peste pupăză, Horton a spus că multe dintre cele peste 40 000 de farmacii on-line ilicite se bazează pe mai mulți furnizori, prin urmare calitatea și siguranța medicamentelor pe care le livrează se pot schimba de la o zi la alta, după cum fluctuează prețurile pe piețele angro și de *dropshipping**.

„Majoritatea acestor programe de farmacii afiliate nu au doar un furnizor, a spus Horton. Unele dintre cele mai mari au zeci de furnizori. De aceea, pentru că un anumit medicament oferit de o rețea apare ca fiind autentic în urma analizelor

* Sistem de livrare directă către client (n. red.).

efectuate într-o zi, nu înseamnă că, data viitoare când îl va comanda cineva, va fi vorba despre același medicament."

După părerea lui Horton însă, motivul cel mai important pentru care nici FDA, nici industria farmaceutică nu au depus eforturi însemnate în vederea efectuării unor analize este acela că ele ar putea arăta că medicamentele vândute de multe așa-numite farmacii ilicite sunt în mare măsură identice din punctul de vedere al compoziției chimice cu cele vândute de farmaciile autorizate.

„Sincer, este un fel de sabie cu două tăișuri, a spus el. Să presupunem că analizezi medicamentele Rx-Promotion și acestea se dovedesc a fi reale, echivalente din punct de vedere chimic cu cele pe care le-ai cumpăra de la o farmacie locală. Nu rezultă atunci că, dând publicității aceste rezultate, susții aproape implicit siteul care a vândut medicamentele respective?"

Din acest motiv, de analiza medicamentelor vândute de farmaciile ilicite se ocupă în mare măsură cercetătorii din învățământul universitar, care încearcă să găsească date despre siguranța și eficacitatea medicamentelor promovate prin spam, care ar trebui eliberate doar pe bază de rețetă. Stefan Savage, profesor la University of California din San Diego (UCSD), a condus o echipă care, timp de câteva luni, în 2011, a făcut peste 800 de comenzi de probă de la farmacii promovate prin e-mail nesolicitat.

„Părerea generală era că aceste farmacii îți iau banii, îți iau datele de pe cardul de credit, iar tu nu te alegi niciodată cu nimic, a spus el. Noi am vrut să știm dacă, atunci când comanzi de la aceste magazine, primești ceva și, în caz afirmativ, de unde vin produsele, cine procesează plățile și așa mai departe."

Savage a spus că a fost surprins să constate că medicamentele pe care le-au cumpărat și le-au analizat păreau să aibă ingredientele active corespunzătoare în cantități aproximativ corespunzătoare, dar nu au putut verifica prezența agenților de contaminare, care ar fi putut pune în pericol sănătatea clienților.

„Din motive legale, nu putem cumpăra toate medicamentele și nici nu suntem dotați pentru a le testa pe toate, a spus Savage. În cele pe care le-am analizat însă, ingredientul activ corespunzător era în cantitatea adecvată. Deci se pare că, într-adevăr, din punctul de vedere al celor implicați în această afacere și al mesajelor pe care și le transmit, ei cred că vând un produs echivalent cu ceea ce clienții pot cumpăra dintr-o farmacie clasică."

În 2012, Savage și colegii săi de la UCSD, împreună cu cercetători de la International Computer Science Institute și George Mason University, au examinat datele financiare ale activităților zilnice desfășurate de GlavMed, SpamIt și Rx-Promotion. A rezultat probabil cea mai detaliată analiză de până acum a epidemiei de malware și spam care persistă până în prezent. Ei au descoperit că clienții fideli sunt esențiali pentru o farmacie ilicită care se dorește a fi rentabilă. Comenzile acestor clienți constituiau 27% din venitul mediu al rețelei GlavMed, respectiv 38% în cazul SpamIt. Pentru Rx-Promotion, venitul adus de aceste comenzi reprezenta până la 23% din venitul total.





„Asta spune câteva lucruri, printre care și faptul că mulți dintre cei care au cumpărat de la rețelele respective au fost satisfăcuți", a comentat Savage, remarcând totuși că destui clienți fideli cumpărau medicamente supuse unor restricții și care cauzează dependență, inclusiv analgezice. „Poate că medicamentele pe care le-au cumpărat au avut un puternic efect placebo, dar bănuiala mea e că aceștia sunt clienți mulțumiți și de aceea au mai făcut comenzi.

De departe, cea mai importantă chestiune legată de medicamentele promovate prin spam se referă la eficacitatea și siguranța lor. Am discutat cu sute de americani care au cumpărat medicamente eliberate pe bază de rețetă de pe siteurile farmaciilor promovate prin SpamIt și am primit o mulțime de

răspunsuri cu privire la eficacitatea lor. Însă niciunul dintre cei cu care am vorbit nu mi-a putut da detalii despre siguranța sau puritatea lor.

Din acest motiv, sperasem să obțin sprijinul chimiștilor și al cercetătorilor. Gary Warner, director de cercetare în domeniul criminalității informatice la University of Alabama din Birmingham (UAB), a încercat să analizeze aceleași aspecte, dar s-a izbit la tot pasul de obstacole birocratice. De aceea, la scurt timp după ce am primit datele de la GlavMed–SpamIt, le-am trimis lui Warner. La rândul său, a încercat să determine diverse companii farmaceutice interesate să folosească acele date pentru a iniția o investigație mai amplă și mai bine finanțată a farmaciilor on-line ilicite, dar eforturile lui n-au avut succes.

Campusul vast al UAB este cunoscut și ca „Universitatea care a Înghițit Birminghamul", iar motivul nu e greu de înțeles. Orașul Birmingham are cu puțin sub 250 000 de locuitori, iar unul din zece este student la universitate.

La etajul al treilea al unei clădiri banale din cărămidă, în centrul campusului, se află laboratorul de criminalistică informatică al UAB, unde Warner petrece opt–zece ore pe zi cu studenți, absolvenți și doctoranzi care, la fel ca mine, par să fie animați de pasiunea de a-i urmări pe băieții răi de pe internet.

Warner stă în fața unei table albe, care acoperă un perete de sus până jos, plină cu ecuații ale unui algoritm matematic pe care încearcă să-l determine cei 20 și ceva de experți din laboratorul de informatică. El arată întruna spre șirurile de servere și computere Mac OS X aflate de o parte și de cealaltă a încăperii închise etanș, cu atmosferă controlată, folosite și de studenții care lucrează în cadrul unui program al Defense Advanced Research Projects Agency (DARPA) pentru a crea și a studia programe malware într-un mediu de laborator.

Dependent de cafeină, lucru pe care nu se sfiește să-l recunoască, Warner soarbe din a treia cutie de Mountain Dew fără zahăr din acea zi. Vorbește înflăcărat despre pericolele

care-i pasc pe cei care comandă de la farmaciile fără licenţă de pe internet, indiferent dacă medicamentele în sine sunt reale şi echivalente din punct de vedere chimic cu cele care pot fi cumpărate din farmaciile clasice.

Una dintre probleme, spunea el, este că multe farmacii fără licenţă de pe internet vând o sumedenie de medicamente a căror utilizare a fost interzisă sau supusă unor restricţii severe în SUA din cauza efectelor secundare periculoase – fără să existe niciun avertisment sau instrucţiuni privind utilizarea lor.

De exemplu, gigantul farmaceutic Roche a decis să-şi retragă medicamentul antiacneic Accutane de pe piaţa SUA după ce instanţele au acordat despăgubiri de milioane de dolari foştilor utilizatori de Accutane. S-a constatat că exista o legătură strânsă între medicamentul respectiv şi apariţia unor malformaţii congenitale la copiii născuţi de femei care îl utilizaseră în timpul sarcinii. Ca urmare, FDA a cerut în 2005 ca Accutane să fie vândut numai femeilor care se angajează să se supună mai multor teste de sarcină şi să folosească minimum două forme de contracepţie pe durata tratamentului. Accutane continuă să fie însă disponibil la farmaciile ilicite de pe internet.

Iată un alt exemplu privind riscurile pe care oamenii şi le asumă când cumpără de la aceste farmacii: ei nu primesc informaţii vitale despre pericolele grave la care se expun dacă iau anumite medicamente în anumite condiţii sau în combinaţie cu alte medicamente. Pe de altă parte, farmaciile legale fac tot ce le stă în putere pentru a se asigura că clienţii lor înţeleg aceste riscuri înainte de a le onora reţetele.

„Multe dintre farmaciile ilicite continuă să facă publicitate unor medicamente suspendate de la vânzare, interzise sau supuse unor restricţii drastice, a spus Warner. În plus, nu îl avertizează pe potenţialul cumpărător cu privire la modul în care ar trebui utilizate aceste medicamente, chiar dacă există condiţii care, în mod normal, sunt aduse la cunoştinţa clientului când cumpără medicamentele respective din farmaciile obişnuite."

Exemplul cel mai evident de risc asociat medicamentelor eliberate de farmaciile din rețelele GlavMed și SpamIt sunt cele două–patru pastile gratuite de Viagra sau Cialis contrafăcute, expediate cu fiecare comandă. Pilulele erau introduse în toate comenzile, chiar și cele de substanțe precum nitrații, care pot avea un efect letal când sunt combinate cu medicamente pentru disfuncția erectilă (DE). Medicii au avertizat de mult timp să nu se ia medicamente DE împreună cu medicamente pentru scăderea tensiunii arteriale, deoarece aceasta ar putea scădea periculos de mult, putând duce la infarct.

Laboratorul de criminalistică informatică al UAB este locul ideal pentru testarea medicamentelor cumpărate prin spam. Un etaj mai jos, dr. Elizabeth Gardner își petrece mare parte a timpului analizând noi „droguri legale". Acestea sunt substanțe halucinogene, create din versiuni sintetice ale unor compuși chimici a căror utilizare și distribuție sunt supuse unor restricții stricte în SUA. Unele dintre aceste droguri legale sunt destul de inofensive – de pildă, pastilele de „creșterea performanței", care se vând și în benzinării, a căror denumire face aluzie la presupusa lor capacitate de a spori rezistența bărbaților în pat.

„Cele mai multe conțin doar multă cofeină și vise deșarte", glumește Gardner.

Există droguri legale mult mai puternice și cu efecte secundare devastatoare, ba chiar îngrozitoare. Chiar înainte de vizita mea în campusul UAB, polițiștii din Miami, statul Florida, au răspuns unui apel de urgență și au fost martorii unei scene care părea desprinsă direct dintr-un film cu zombi de la Hollywood. Ei au fost chemați într-un loc aflat pe o șosea, sub o pasarelă, unde se petrecuse o agresiune. Sosind la locul faptei, polițiștii au împușcat și au ucis un localnic de 31 de ani, care a fost găsit mâncând fața unui om fără adăpost în plină zi. Anchetatorii au descoperit ulterior că atacatorul se transformase într-un adevărat zombi după ce ingerase cantități

importante de „săruri de baie", un stimulent sintetic conceput pentru a produce efecte similare cu amfetaminele și cocaina.

Este joi după-amiază, la jumătatea lunii iunie a anului 2012, iar Gardner face analiza unui eșantion de săruri de baie. Fragmente din acestea sunt introduse într-o cutie mare, albă, care seamănă cu o imprimantă laser supradimensionată. Dispozitivul este un spectrometru de mase, folosit pentru a căuta și a identifica ingredientele active ale diverselor substanțe. Aproape fără zgomot, acesta analizează în mod automat câteva eprubete minuscule, pline cu substanțe chimice.

Aparatul produce date care sunt transmise unui computer. Acesta le utilizează pentru a trasa un grafic pe care se pot vedea câteva linii frânte foarte înalte.

„Vezi creșterile astea? spune Gardner, arătând două vârfuri foarte înalte. Sunt markerii chimici ai mefedronei, care este ingredientul activ al acestor săruri."



În ciuda eforturilor depuse, nu am putut convinge pe niciunul dintre cumpărătorii de medicamente on-line să-mi trimită câteva pastile pentru a fi analizate de laboratorul lui Gardner. Nu că ar fi contat: oricum, UAB nu a primit autorizație să facă așa ceva.

Este incredibil faptul că cercetătorii de la UAB au primit de la autoritățile federale autorizația de a analiza și de a lucra cu substanțe ilegale, supuse unor restricții severe, ca heroina, cocaina și o metamfetamină, dar n-au primit încă aprobarea FDA și DEA pentru a putea analiza medicamente comandate prin e-mail nesolicitat.

Una dintre probleme este aceea că, în 2008, Congresul SUA a schimbat legislația, promulgând Legea Ryan Haight, care specifică în mod expres faptul că este ilegal să comanzi pe internet medicamente eliberate pe bază de rețetă medicală dacă nu ai acea rețetă. În plus, chiar dacă un american are o rețetă valabilă pentru un medicament, este ilegal să-l comande de la o farmacie din afara SUA, care să-l expedieze apoi în SUA.

„Problema este ca și rezolvată, a spus Warner. Avem protocoalele de acord, avem deschise căsuțele poștale și avem aprobarea conducerii universității. Mai avem de trecut acest mic obstacol administrativ." Deocamdată, nu aveau acordul autorităților federale.

Warner apelase chiar la ajutorul unei bănci regionale, dispuse să pună la dispoziția cercetătorilor carduri preplătite, care puteau fi folosite pentru a cumpăra medicamente de la GlavMed–SpamIt și Rx-Promotion.

„Banca e dispusă să susțină operațiunile noastre, dar ne mai trebuie un act guvernamental oficial, în care să se specifice în esență că nimeni nu va face închisoare pentru asta", a spus Warner. Era planificat ca universitatea să primească o subvenție de la FDA pentru a efectua cercetări asupra farmaciilor ilicite, dar autoritățile puneau condiții serioase.

„În principiu, au spus că banii nu vor putea fi utilizați pentru cumpărarea de medicamente, iar dacă vor fi folosiți pentru analiza medicamentelor comandate prin spam, atunci subvenția va fi retrasă, a spus Warner. Ce s-a schimbat între momentul când FDA a propus acordarea finanțării și momentul precizării acestor condiții? Nu se știe. Au spus doar: «Nu este legal să vă autorizăm să cumpărați medicamente.» Ca atare, FDA a trebuit să revină și să acorde subvenția doar pentru evaluarea siteurilor din e-mailurile nesolicitate, fără a mai avea dreptul să cumpărăm medicamente."

Nu era pentru prima dată când Warner și UAB au fost împiedicați în încercările lor de a testa medicamente comandate prin spam. Cu puțin timp înainte de a-i transmite datele de la GlavMed, Warner a avut o întâlnire cu directorii și specialiștii de la Pfizer care investigau cazurile de fraudă. Gigantul farmaceutic a lăsat să se înțeleagă faptul că era interesat să colaboreze cu UAB la realizarea unui studiu cu privire la medicamentele achiziționate prin intermediul rețelelor de farmacii ilicite. La urma urmelor, vânzările de Viagra

contrafăcută, cel mai bine vândut medicament al său, reprezentau peste 40% din totalul tranzacțiilor realizate de Rx-Promotion și GlavMed.

Finanțarea unui astfel de proiect era însoțită însă și de anumite condiții.

„Cei de la Pfizer au spus că vor să colaboreze cu noi la acest proiect atâta vreme cât aveau dreptul să-l oprească dacă s-ar fi dovedit că medicamentele erau autentice, își amintea Warner. Microsoft discuta cu noi și cu Pfizer dacă UAB și Microsoft ar putea crea un site, de genul pilldangers.org, care să-i avertizeze pe oameni despre pericolele cumpărării de medicamente de pe internet. Iar chimistul meu a întrebat: «Dar dacă medicamentele sunt autentice?» La care reprezentantul lui Pfizer a zis: «Atunci n-am vrea să mai publicăm nimic.» Le-am spus că noi, profesorii, punem un accent foarte mare pe libertatea de exprimare și că nu vom putea accepta această condiție. I-am spus că am putea să zicem, de exemplu: «În 25% dintre cazuri, am primit medicamente reale.» Atunci, respectivul a zis: «Nu, nu, nu puteți face așa ceva. Vrem să dați publicității doar ce ați constatat în cazul medicamentelor contrafăcute.»"



Apoi, după ce a primit datele de la GlavMed, Warner a vorbit cu un alt Warner – Mark Warner, directorul departamentului de informații de la Pfizer, care lucrase 21 de ani în FBI. Warner de la UAB a spus că Warner de la Pfizer l-a sunat pentru a discuta despre o posibilă colaborare privind analiza datelor de la GlavMed în vederea obținerii de informații pe care autoritățile americane să le poată prezenta după aceea rușilor pentru a-i ajuta să stopeze valul de spam care afecta lumea.

„Am terminat discuția telefonică cu el înainte să fi înțeles exact cine era, dar se comporta ca un polițist necioplit, de modă veche, își amintea Warner de la UAB. Este newyorkez, așa că discuția s-a desfășurat cam așa: «Ascultă-mă pe mine, dom'le Warner. Eu m-ocup de chestii de-astea de mai mult

timp ca tine. Uite care-i treaba: rușii n-o să facă nici pe naiba pentru noi. Noi trebuie să-i găsim pe afiliații spam care sunt în SUA și să-i arestăm. Poți să uiți de ruși. N-o să ne putem atinge de ei niciodată. Rușii sunt blindați. Nu-i putem atinge. Hai mai bine să-i găsim pe tipii din SUA, să-i băgăm la zdup și să mergem mai departe.»"

Pe de o parte, Warner de la Pfizer avea dreptate: conform celor mai mulți experți în legislație cu care am discutat când am scris această carte, nu exista aproape nicio șansă ca rușii *să facă* ceva. În primul rând, hackerii din Rusia sunt, în general, lăsați în pace atât timp cât nu fură de la companiile sau cetățenii ruși. Dar Warner de la UAB a spus că fusese surprins de răspunsul primit. La urma urmelor, peste 40% dintre vânzările realizate de GlavMed implicau versiuni contrafăcute de Viagra, marele succes de piață al companiei Pfizer, așa că ar fi fost în interesul ei să colaboreze.

„Pur și simplu nu-mi venea să cred ce mentalitate de troglodit avea individul acela, a spus Warner într-o discuție telefonică. M-am gândit că, chiar dacă a lucrat 21 de ani în FBI, nu înseamnă că știe ceva despre criminalitatea informatică. În același timp, versiunile contrafăcute ale celui mai vândut produs al companiei lui erau medicamentul cel mai bine vândut de GlavMed. Ei ar fi cei mai în măsură să se plângă de spamul farmaceutic, dar cine știe? Poate că profitul de 100 de milioane de dolari adus de produsele SpamIt și GlavMed contrafăcute nu înseamnă nimic pentru o companie care câștigă zeci de miliarde anual."

Warner de la UAB a spus că se simțea tot mai mult cuprins de disperare știind că avea atât de multe informații despre o uriașă conspirație în domeniul criminalității informatice, iar autoritățile nu păreau interesate să folosească datele existente.

„Participasem la grupul de lucru al FBI în domeniul fraudei farmaceutice și eram foarte dezamăgit de faptul că aproape niciuna dintre marile companii farmaceutice nu venise la

întâlniri, a spus el. Cel puțin la întâlnirile la care am participat, erau vreo șapte companii farmaceutice, dar nu auzisem despre niciuna dintre ele. Roche nu venise, Bayer nu venise, Pfizer nu venise. Merck nu venise. Parcă AstraZeneca a venit la una dintre întâlniri. Dar n-am putut stârni interesul nimănui."

Acestea fiind spuse, s-ar putea să fi existat un alt motiv pentru care Pfizer nu intenționa să ajute FBI-ul. Cu puțin timp înainte ca Warner să obțină datele despre GlavMed–SpamIt, FBI încheiase o anchetă penală în cazul companiei Pfizer pentru promovarea utilizărilor neautorizate ale medicamentelor sale cu vânzările cele mai mari și pentru acordarea de comisioane medicilor în vederea promovării lor. Guvernul a declarat că agenții de vânzări ai companiei Pfizer făcuseră afirmații înșelătoare despre utilizarea medicamentelor firmei. De exemplu, se spunea că acestora li s-ar fi cerut să-i învețe pe medici cum să discute cu femeile pentru a le prescrie Viagra celor care aveau dificultăți în atingerea orgasmului.



Pfizer a negat acuzațiile, dar a acceptat soluționarea amiabilă a litigiului pentru suma de 2,3 miliarde de dolari, aceasta fiind, în acel moment, cea mai mare sumă plătită vreodată Departamentului de Justiție al SUA într-un caz de înșelăciune. Ea echivala cu veniturile anuale realizate de Pfizer din vânzările de Viagra. Nu e de mirare că gigantul farmaceutic nu a dorit să atragă FBI-ul în altă investigație, chiar dacă aceasta ar fi fost în beneficiul său.

În ceea ce o privește, compania Pfizer a ales să deschidă procese civile împotriva spammerilor și falsificatorilor. În ultimii cinci ani, ea a cheltuit milioane de dolari cu investigarea și plata unor taxe juridice pentru a-i aduce în instanță pe furnizorii de Viagra contrafăcută și alte medicamente false. (Reprezentanții Pfizer au refuzat solicitările mele repetate de a sta de vorbă pentru această carte.)

Warner era dezamăgit că nu putea obține permisiunea de a analiza medicamentele pe bază de rețetă achiziționate de

la Rx-Promotion și GlavMed–SpamIt. Părea să spere totuși că bazele de date cu privire la clienții ambelor afaceri vor fi suficiente pentru a contribui la descurajarea unora dintre cei mai mari spammeri și botmasteri din lume, care lucrau aproape toți pentru cel puțin una dintre aceste rețele de farmacii afiliate și ale căror date personale și financiare apăreau în toate documentele sustrase de la acestea.

Același activist care-mi transmisese baza de date GlavMed a spus că a trimis o copie a ei și unor contacte din FBI. Timp de câteva săptămâni, la sfârșitul anului 2010, mai multe agenții guvernamentale s-au luptat între ele ca să preia investigația respectivă. În cele din urmă, s-a hotărât ca ancheta să vizeze încălcarea drepturilor de proprietate asupra mărcii comerciale și a fost încredințată unei unități operative a Biroului pentru imigrație și aplicarea reglementărilor vamale din cadrul Departmentului Securității Interne.

Această unitate operativă, denumită National Intellectual Property Rights Coordination Center (NIPR), folosește, în vederea realizării anchetelor civile și penale, resursele a cel puțin 20 de agenții, printre care FBI, Interpol, US Postal Inspection Service, National Aeronautics and Space Administration (NASA) și Royal Canadian Mounted Police.

Ancheta NIPR a făcut parte dintr-o încercare mai amplă a administrației Obama de a stopa abuzurile legate de drepturile de proprietate intelectuală on-line, inclusiv vânzările farmaciilor ilicite și comerțul ilegal cu filme, muzică și software piratate. Cam în aceeași perioadă, reprezentanții administrației au anunțat rezultatele operațiunii „Pangea", o acțiune anuală a Interpol îndreptată împotriva criminalității farmaceutice. Operațiunea, care a durat o săptămână, a dus la închiderea a cel puțin 290 de farmacii on-line ilicite, confiscarea a aproape 11 000 de pachete conținând peste un milion de pastile și arestarea sau cercetarea a cel puțin 76 de persoane asociate cu farmaciile.

Multe dintre siteurile închise în urma operațiunii „Pangea" au fost magazine promovate de spammeri care lucrau pentru programul Rx-Promotion al lui Vrublevski. Chiar înainte de a fi închise, US Food and Drug Administration a trimis o scrisoare partenerului lui Vrublevski, Iuri „Hellman" Kabaienkov, anunțându-l că a identificat 294 de siteuri care vindeau medicamente strict controlate, ce se eliberau doar pe bază de rețetă și creau dependență, precum analgezicele, fără să solicite rețeta. Se părea că autoritățile americane începuseră în sfârșit să ia poziție.

În esență, cei de la Rx-Promotion au ridicat din umeri. Potrivit lui Vrublevski, aproape nimeni din companie n-a observat închiderea siteurilor. În mod paradoxal, numărul acestora a fost mai mult sau mai puțin egal cu numărul mediu al siteurilor care dispăreau săptămânal ca urmare a eforturilor regulate de curățare întreprinse de grupările antispam și companiile de găzduire web.





„A fost foarte amuzant să citesc știrile și să văd că a existat operațiunea aceasta uriașă, internațională, care a dus la închiderea a sute de farmacii ilegale de pe internet, a spus Vrublevski. Apoi intri pe forumuri de spammeri și hackeri și-i vezi că se întreabă unii pe alții: «Nenică, tu ai simțit asta?» sau «nenică, tu ai observat asta?» Nu mi s-a părut că i-ar fi păsat cuiva sau că cineva ar fi observat măcar."

Vrublevski spunea că, în săptămânile anterioare operațiunii, reprezentanții unui grup de firme americane – mai cu seamă deținătoare de drepturi de autor din industria divertismentului – avuseseră o întâlnire cu membrii Dumei de Stat, camera inferioară a parlamentului rus. Întâlnirea a făcut parte dintr-o campanie a industriei de divertisment desfășurată în Rusia în vederea stăvilirii pirateriei în domeniul muzicii și al filmelor. Sloganul campaniei se traducea aproximativ „Spuneți «nu» hoților!".

E-mailurile scurse de la ChronoPay arată că firma respectivă plătea în mod discret cel puțin un membru al Asociației

Ruse a Comunicațiilor Electronice (ARCE), un grup din industria de profil. Potrivit facturilor ChronoPay, compania a achitat „o taxă lunară pentru consultanță în relații publice" – respectiv 16 666,66 de euro – lui Dmitri Zaharov, pe atunci director pentru relații publice la ARCE. (Aceasta era altă datorie pe care Vrublevski și ChronoPay n-o onoraseră. Arhiva ChronoPay este plină de mesaje de la recuperatorii de creanțe ai ARCE, care trăgeau, fără succes, de reprezentanții ChronoPay să plătească zeci de mii de euro drept taxe de „consiliere" datorate.) Am cerut un comentariu din partea domnului Zaharov despre acest aranjament, dar n-am primit niciun răspuns. A fost un lucru frustrant și paradoxal, și pentru că Zaharov a părăsit ARCE în 2010, iar acum este director adjunct al Departamentului de comunicații externe din Ministerul Telecomunicațiilor și Comunicării în Masă din Rusia.

Într-o convorbire telefonică avută la o lună după operațiunea „Pangea", Vrublevski mi-a spus că i-a contactat pe conducătorii ARCE ca să-i ia peste picior pentru participarea la forumul dedicat drepturilor de autor și mărcilor comerciale.

Cum era de așteptat, proprietarii drepturilor de autor – în special din industria cinematografică – au amenințat membri ai ARCE, precum Vkontakte (o versiune în limba rusă a Facebook) și mail.ru (furnizor de servicii de webmail), că vor apela la autorități dacă nu vor elimina toate materialele care încălcau drepturile de autor. Vrublevski a spus: „Am auzit de asta, i-am sunat pe tipii de la ARCE și le-am zis: Băi, câtă minte vă trebuie ca să nu vă duceți la o întâlnire cu deținătorii de drepturi intitulată «Spuneți nu hoților»?"

Ulterior, în cursul anului 2010, ARCE a trimis o scrisoare oficială Victoriei Espinel, cea care se occpa de drepturile de proprietate intelectuală din partea administrației Obama. Prin această scrisoare – care a fost trimisă și celor de la Google, Microsoft, National Association of Boards of Pharmacy și LegitScript – se oferea ajutor industriei rusești de înaltă tehnologie

pentru a combate spamul și a susține viitoarele inițiative menite să elimine farmaciile ilicite de pe internet.

În scrisoare se susținea că pierderea economică provocată în Rusia de spam a fost de 450 de milioane de dolari în 2009 și că, de aceea, Rusia se străduia să elaboreze propriile legi antispam. ARCE n-a menționat că unul dintre fondatorii farmaciei de pe internet vizate de recenta operațiune „Pangea" a guvernului american era șeful comisiei guvernului rus responsabile cu formularea de recomandări privind elaborarea acelor legi antispam.

În încheierea scrisorii, reprezentanții ARCE se ofereau să găzduiască o videoconferință cu circuit închis cu reprezentanți ai administrației Obama și ai industriei de înaltă tehnologie, „în cadrul căreia să discutăm despre rezultatele disponibile ale cercetărilor, problemele actuale, inițiativele și posibilitățile de acțiuni comune dedicate stabilizării situației în domeniul criminalității informatice în general și al spamului farmaceutic în special".





Președintele LegitScript, John Horton, a spus că, imediat după ce a primit un exemplar al scrisorii, i-a contactat pe cei de la FDA și pe Espinel.

„Le-am spus: «Sunt sigur că știți ce se-ntâmplă cu ChronoPay» și a reieșit că știau, a zis Horton. De asemenea, i-am trimis un e-mail Victoriei [Espinel] și i-am spus că părerea mea neoficială era să nu răspundă la scrisoare."

La mijlocul lunii august a anului 2010, Andrew J. Klein, consilier al președintelui Obama în domeniul drepturilor de proprietate intelectuală, i-a invitat pe șefii companiilor care alocă numele domeniilor de pe internet și ai celor care administrează bazele de date cu domeniile de pe internet să participe la o întâlnire de trei ore la Casa Albă pentru a discuta despre posibilitățile de închidere forțată a siteurilor care vând medicamente contrafăcute, eliberate pe bază de rețetă.

Invitația a fost trimisă prin e-mail către zeci de directori și juriști ai unora dintre cele mai mari companii de internet

din lume, printre care Google, Microsoft, PayPal, Visa și Yahoo! Destinatarii au fost invitați să participe, la 29 septembrie, la o întâlnire cu reprezentanți ai Casei Albe și guvernului, inclusiv cu Victoria Espinel.

„Obiectivul acestei întâlniri", se afirma în invitație, „este de a discuta despre activitățile ilegale care au loc pe internet în general și, mai concret, despre încheierea unor acorduri cu privire la problema vânzării ilegale on-line de medicamente contrafăcute, care necesită rețetă, nesupuse restricțiilor."

Mai mulți participanți la eveniment l-au catalogat mai degrabă o ambuscadă decât o întâlnire a unor persoane inteligente dornice să rezolve o problemă dificilă și au spus că, în esență, Espinel le declarase participanților că trebuiau să găsească neapărat o soluție voluntară.

„În principiu, ea a adunat câțiva proprietari ai unor branduri importante pentru a le spune: «Trebuie să faceți ceva în privința asta, fiindcă altfel vi se va face vouă ceva»", a spus Savage de la UCSD, rememorând o discuție avută cu un participant.

Puțini știau în acel moment că una dintre firmele invitate – Google – era deja cercetată penal de Departamentul de Justiție al SUA deoarece căutase să convingă farmacii canadiene false – inclusiv multe farmacii ilicite de pe internet create de SpamIt și Rx-Promotion – să facă publicitate medicamentelor destinate distribuirii în SUA.

Implicațiile acestui caz erau uriașe. Una dintre modalitățile în care farmaciile afiliate la GlavMed își promovau siteurile era spargerea altor siteuri. Ele introduceau în siteurile sparte zeci de linkuri și chiar pagini de web întregi, care îi redirecționau pe vizitatori către siteuri ce comercializau medicamente contrafăcute, eliberate pe bază de rețetă. Cu cât farmaciile afiliate îndreptau mai multe siteuri legitime spre propriile magazine, cu atât acestea din urmă ocupau o poziție mai bună în rezultatele principalelor motoare de căutare când utilizatorii căutau

anumite medicamente. Acest proces – denumit în lumea subterană „optimizare neagră a motoarelor de căutare" – a fost un important factor determinant al vânzărilor realizate de farmaciile afiliate atât la Rx-Promotion, cât și la GlavMed–SpamIt.

Era destul de rău că rezultatele căutărilor pe Google erau în mod constant compromise de spammeri. Luând însă bani de la farmacii on-line nereglementate, potențial afiliate spammerilor, Google întrecea orice limită. Potrivit Departamentului de Justiție al SUA, Google știa încă din 2003 că farmaciile canadiene expediau în mod ilegal în SUA medicamente eliberate doar pe bază de rețetă.

Google avea să aranjeze mai târziu lucrurile, acceptând să plătească o impresionantă amendă de 500 de milioane de dolari. A fost una dintre cele mai mari amenzi achitate vreodată Departamentului de Justiție, dorindu-se ca ea să echivaleze cu veniturile obținute de companie din publicitatea făcută farmaciilor canadiene și cu veniturile pe care farmaciile respective le-au obținut de la clienții americani care au cumpărat medicamente supuse restricțiilor.



La mai puțin de două luni după întâlnirea de la Casa Albă, Espinel a participat la o conferință de presă. Flancată de procurorul general al SUA, Eric Holder, și de Janet Napolitano, pe atunci secretar al Departamentului Securității Interne, Espinel a anunțat crearea unei noi organizații nonprofit care să lupte împotriva farmaciilor ilicite de pe internet.

„Un grup de parteneri din sectorul privat a anunțat astăzi că va forma o nouă organizație nonprofit cu scopul de a colabora atât între ei, cât și cu guvernul american în vederea eliminării de pe internet a farmaciilor ilegale", a explicat Espinel, numindu-i apoi pe membrii organizației nonprofit: American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, Network Solutions, Neustar, PayPal, Visa și Yahoo.

„Acest grup de companii a făcut un pas extraordinar, fără precedent în combaterea farmaciilor on-line ilegale, a spus Espinel într-o sală plină cu reporteri și camere TV. Credem că

această acțiune va avea un efect rapid și semnificativ asupra farmaciilor on-line ilegale, schimbând regulile și făcând cunoscut faptul că firmele legitime nu vor interacționa cu răufăcătorii."

Anunțul făcut avea o singură problemă. Puține persoane din conducerile companiilor numite își aminteau să fi fost de acord cu formarea unei astfel de organizații nonprofit.

„Înainte de conferința de presă, reprezentanții companiilor respective au participat la o masă rotundă pentru a discuta despre ea, dar nimeni n-a avut intenția de a accepta să formeze grupul respectiv, a spus Warner. Cei cu care am stat de vorbă și care au urmărit conferința de presă la care se anunțase că fuseseră de acord să formeze acel grup au plecat de acolo întrebându-se: «Am făcut noi asta?»"

La un an și jumătate de la crearea organizației nonprofit, anunțată pentru prima dată de Espinel la conferința de presă de la Casa Albă, membrii acesteia nu se întâlniseră încă niciodată. În aceeași perioadă era închis cazul NIPR. Avertismentul șefului securității de la Pfizer avea să se dovedească ciudat de profetic. Potrivit surselor din două agenții federale, care au cerut să nu fie numite deoarece nu erau autorizate să dea declarații oficiale, ancheta cu privire la spammerii și hackerii angajați de GlavMed și SpamIt a fost abandonată și fiindcă se considera că majoritatea făptașilor se aflau în Rusia și în foste țări sovietice, care, de regulă, erau mai puțin cooperante cu autoritățile occidentale care urmăreau să pună mâna pe infractorii informatici de pe teritoriul lor.

Ținând seama de lipsa de interes a autorităților federale față de analiza metodică a medicamentelor comandate de la aceste farmacii ilicite lipsite de scrupule, rămâne neclar dacă majoritatea acestor medicamente conțin ingrediente active în cantități adecvate, fără substanțe nocive care i-ar putea afecta sau chiar ucide pe cei care le ingeră.

Această inacțiune pare să convină industriei farmaceutice, care se ferește să analizeze și să obțină rezultate ce ar putea indica faptul că marea majoritate a medicamentelor

comandate prin spam sunt mult mai ieftine și la fel de sigure ca medicamentele cumpărate de la farmaciile clasice.

Din păcate, lipsa unor date obiective despre siguranța și eficacitatea medicamentelor cumpărate prin intermediul spamului nu contribuie la scăderea cererii, consumatorii fiind în continuare expuși la o periculoasă ruletă rusească.

# Capitolul 6

# PARTENER ÎN CRIMA (DEZ)ORGANIZATĂ





Un citat faimos din *Arta războiului* de Sun-tzu se aplică perfect cercetărilor şi motivaţiei mele de a scrie această carte: „Cunoaşte-ţi duşmanul." După ce am aflat într-o oarecare măsură ce anume motivează farmaciile care depind de spam şi pe clienţii lor, a sosit timpul să examinez cum funcţionează de fapt operaţiunile de spam. Forţa motrice din spatele succesului unor programe ca Rx-Promotion şi GlavMed – şi motorul care propulsează practic toate eforturile de colaborare din criminalitatea informatică – este un aranjament numit în Rusia *partnerka*, care înseamnă literalmente „parteneriat". *Partnerka* precum GlavMed şi Rx-Promotion urmăresc să combine companii dubioase care-şi fac reclamă cu firme dispuse să cumpere traficul web care poate fi generat prin spam.

Multe companii legitime care caută să atragă mai mulţi clienţi – în special firme mici din Rusia şi Europa de Est – vor încerca să sporească gradul de cunoaştere de către publicul consumator a produselor sau serviciilor lor şi cererea pentru acestea prin angajarea unui spammer. Deşi utilizarea unor computere accesate în mod neautorizat pentru trimiterea de e-mailuri nesolicitate este teoretic ilegală în Rusia, multe companii legitime ruseşti nu au habar de această interdicţie sau nu se tem de ea.

Aşa cum vom vedea în capitolul 7, „Vergiliu" al nostru din lumea subterană a spammerilor – Igor Vişnevski, finanţatorul botnetului Cutwail – şi-a început activitatea în acest domeniu când şeful i-a ordonat să găsească un mod de a atrage mai mult trafic spre siteul companiei sale.

De fapt, atunci când botnetul Cutwail este folosit pentru a expedia spam la adresele de e-mail care se termină în „.ru", mesajele conţin frecvent un număr de telefon din Rusia, la care destinatarii pot suna spre a se interesa despre ce trebuie să facă dacă vor să comande reclame spam pentru propriile produse şi servicii.

„Am văzut promovate în felul ăsta aproape tot ce-ţi poţi închipui, de la ţigări electronice la clădiri pentru birouri şi hoteluri", a spus Brett Stone-Gross, cercetător la University of California, care a studiat multă vreme funcţionarea botnetului Cutwail.



Într-o *partnerka* de spam, conducătorii operaţiunii – sponsorii – îşi asumă responsabilitatea de a coordona şi de a se ocupa de aproape toate aspectele afacerii, de la conţinutul web la asistenţa oferită clienţilor, negocierile cu furnizorii şi configurarea serverelor web şi a numelor domeniilor pe care urmează a se face publicitate produsului oferit.

Singurul rol al spammerilor (numiţi uneori „adverts" sau „traffers") este acela de a direcţiona trafic către siteurile care vând produsele promovate în spam, putându-se retrage din afacere oricând. Spammerii sunt plătiţi de obicei cu comisioane ce reprezintă între 30% şi 35% din totalul vânzărilor generate de traficul lor. Pentru ei este o afacere destul de profitabilă, cu condiţia ca traficul să genereze clienţi plătitori.

Această dinamică a sistemelor *partnerka* le permite sponsorilor să se ţină la distanţă (cel puţin teoretic) de aspectele mai ilicite ale afacerii – care utilizează de obicei mii de PC-uri controlate neautorizat pentru a expedia mesaje spam şi pentru a găzdui siteurile farmaciilor. Spammerii beneficiază de pe

urma acestui aranjament prin faptul că se pot retrage repede dintr-un program în favoarea altuia care poate oferi condiții mai atractive – de exemplu, comisioane mai mari, asistență mai bună pentru clienți și o varietate mai mare de produse – ce sporesc probabilitatea de a atrage clienți prin spam. În plus, există multe tipuri de parteneriate: cele care promovează replici ale unor ceasuri de marcă, pornografie, poșete de lux contrafăcute și antiviruși falși, ca și spam farmaceutic. Când mesajele nesolicitate apar în contul de e-mail sau sunt oprite de firewall, de filtrul de spam sau de antivirus, ele provin probabil de la una dintre aceste *partnerka*.

Experților în domeniul securității și tehnologiei le place să numească fenomenul *partnerka* „criminalitate informatică organizată". Dar, conform lui Stefan Savage de la UCSD, sistemele *partnerka* pot fi descrise mai exact drept „criminalitate dezorganizată" – adică rețele vag constituite, alcătuite din contractori independenți, interesați în principiu de câștig pentru sine și care rămân în parteneriat doar atâta vreme cât acesta este viabil din punct de vedere economic și competitiv.

„Este într-adevăr un excelent model de afaceri din ambele puncte de vedere, a spus Savage, care a colaborat la mai multe studii pe termen lung despre diverse aspecte ale fenomenului *partnerka*, de la spam la botneturi. Pe de o parte, afiliatul nu trebuie să învețe multe lucruri, cum ar fi procesarea plăților, ci trebuie doar să caute să obțină trafic. De asemenea, are o flexibilitate foarte mare – dacă un parteneriat se desființează sau există altul care plătește mai bine, poți pleca oricând. Modelul *partnerka* oferă așadar o mobilitate incredibilă afiliatului, care nu este legat de nimic."

Savage spunea că programele *partnerka* în sine beneficiază de pe urma aranjamentului prin faptul că nu trebuie să-și asume riscul de a fi asociate teoretic cu botneturile și alte mijloace ingenioase, dar potențial dăunătoare (și dubioase din punct de vedere legal) pe care le pot inventa spammerii pentru a genera trafic.

„Programul iese în câștig, deoarece nu trebuie să mizeze pe modul cel mai bun de a genera trafic, a spus el. Cel care gestionează programul își spune: «Majoritatea tipilor ăstora [spammerii] nu vor obține nimic, dar mie nu-mi pasă pentru că plătesc doar comision. Cineva tot va reuși, iar atunci eu voi obține un câștig frumos.»"

De asemenea, datorită dinamicii sistemului, majoritatea spammerilor nu sunt loiali unui anumit program. De exemplu, aproape toți spammerii de top care lucrează pentru GlavMed și Rx-Promotion fac parte din cel puțin alte șase *partnerka*, printre care EvaPharmacy, Bulker.biz, Rx-Partners și Mailien. Această dinamică reprezintă probabil cea mai frustrantă problemă pentru activiștii antispam care încearcă să oprească fluxul de e-mailuri nesolicitate. Așa cum, dacă apeși pe un balon plin cu aer, acesta nu se face mai mic, ci doar se umflă mai mult într-o parte, campaniile antispam care duc la închiderea unei *partnerka* sau unei componente majore a operațiunii respective îi determină adesea pe afiliații cu cel mai mare succes să-și mute pur și simplu traficul de spam la alte *partnerka*.




Așa cum menționa Dmitry Samosseiko, expert în securitate la SophosLabs Canada, în studiul de referință intitulat „The Partnerka – What Is It, and Why Should You Care?", toate *partnerka* sunt într-o intensă concurență reciprocă.

„Fidelitatea, scria Samosseiko, se dobândește prin plata unor comisioane mai generoase, perioade mai scurte de «așteptare», asistență pentru o gamă mai largă de metode de plată, materiale promoționale de calitate superioară, suport mai bun etc." În mod obișnuit, o *partnerka* plătește comisioanele afiliaților după una–două săptămâni, pentru a nu fi nevoită să-i plătească în același timp pe toți și a se asigura în același timp că ei nu primesc comisioane pentru tranzacții anulate ulterior de procesatorii de carduri de credit.

Samosseiko spunea că *partnerka* folosesc frecvent concursuri și alte trucuri pentru a atrage mai mulți afiliați

(spammeri). „Multe organizează petreceri scumpe pentru membrii lor, le trimit cadouri generoase de sărbători, organizează loterii la care se poate câștiga o mașină de lux și așa mai departe", scria el.

Aceste stimulente cresc și cantitatea de spam pe care o primim. De exemplu, în 2008, Stupin și Gusev – fondatorii și administratorii lui GlavMed și SpamIt – au decis să finanțeze un concurs destinat spammerilor proprii, cu premii considerabile în bani pentru cei al căror spam genera numărul cel mai mare de tranzacții. Fiecare participant a primit o listă cu aproximativ 20 000 de adrese de e-mail, iar concursul a început la 4 iulie 2008, Ziua Independenței SUA.

Primii trei clasați au primit premii cuprinse între 1 000 și 3 000 de dolari, precum și statutul de „Master of Inbox" pe Spamdot.biz, un forum exclusivist deținut de administratorii SpamIt. (Câștigătorul concursului, hackerul rus „Engel", s-a aflat, se pare, în spatele botnetului de spam Festi, o mașină extrem de virulentă și puternică de propagare a spamului, descrisă în amănunțime în capitolul 7. În cele din urmă, Engel și botnetul lui aveau să-l catapulteze pe Vrublevski și pe el însuși spre o coliziune periculoasă cu legea, așa cum vom vedea în capitolul 12.)

În studiul de referință intitulat „PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs", cercetătorii de la University of California din San Diego (UCSD), International Computer Science Institute și George Mason University au examinat datele cu privire la situația financiară zilnică a rețelelor GlavMed, SpamIt și Rx-Promotion, care au procesat în patru ani comenzi de peste 170 de milioane de dolari de la clienți aflați în căutarea unor medicamente mai ieftine, mai accesibile și pe care să le poată procura într-un mod mai discret.

Rezultatul este probabil cea mai detaliată analiză făcută până acum afacerii cu malware și epidemiei persistente de spam. Cercetătorii au ajuns la concluzia că spamul – și toate

relele inerente acestuia – va fi în continuare o problemă supărătoare întrucât cererea consumatorilor pentru produsele cel mai frecvent promovate prin e-mail nesolicitat rămâne constantă.

„Piața pentru medicamentele promovate prin spam nu este nici pe departe saturată, spunea profesorul Stefan Savage de la UCSD. Numărul clienților noi pe care aceste programe și-l fac zilnic explică de ce oamenii deschid mesajele de acest gen. Întrucât expedierea de spam către toți utilizatorii de pe planetă asigură permanent clienți noi, spamul nu va dispărea."

Afiliații înțeleg perfect acest lucru și, la fel ca dealerii regionali de medicamente care revendică părți importante din teritoriul on-line, se ceartă frecvent între ei din invidie, dușmănie sau ca să se răzbune pentru niște ofense închipuite. Aceste războaie teritoriale virtuale se pot transforma repede în conflicte neplăcute și costisitoare pentru toți cei implicați. Acest lucru este valabil mai ales când apar dispute între *partnerka* concurente, deoarece majoritatea afiliaților importanți sunt spammeri de succes, care dispun de botneturi foarte puternice.



Disputele de acest fel sunt scumpe și din cauza costurilor de oportunitate implicate. Atacurile distrugătoare sunt efectuate prin intermediul botneturilor, prin folosirea unor resurse care, în mod obișnuit, sunt utilizate pentru a expedia spam în scopul difuzării de mesaje nesolicitate până când siteul vizat este copleșit și nu mai poate găzdui vizitatori legitimi (adică potențiali cumpărători).

În studiul intitulat „PharmaLeaks", cercetătorii de la UCSD au afirmat că 10% dintre afiliații cu cele mai mari câștiguri au avut o pondere de 75–90% în veniturile totale ale rețelei în toate cele trei programe afiliate.

„Subminarea activităților câtorva afiliați ar avea un efect considerabil asupra profiturilor unui întreg program", au scris cercetătorii.

Șefii obscuri ai diverselor programe *partnerka* au considerat de la început această slăbiciune ca fiind o problemă

existențială. Pentru a remedia situația, ei au încercat să creeze un cartel virtual al parteneriatelor de farmacii on-line, cu scopul de a împiedica izbucnirea unor dispute între *partnerka*, a unor războaie ale prețurilor și migrarea afiliaților între programele farmaceutice fără un anunț prealabil. Șefii *partnerka* credeau că asta va reduce cheltuielile generale și va preveni scăderea episodică a volumului global de spam, asigurând în cele din urmă un flux aproape constant de mesaje nesolicitate spre toate conturile de e-mail.

În acest scop, la 4 septembrie 2007, Dmitri Stupin i-a spus partenerului său, Igor Gusev, că ar vrea ca SpamIt și GlavMed să formeze un cartel farmaceutic cu alte programe *partnerka*. O săptămână mai târziu, Gusev a stabilit o întâlnire pentru a discuta despre această idee cu Leonid Kuvaiev, spammer condamnat și coadministrator al Rx-Partners, un program de spam farmaceutic concurent.

Cam tot atunci, se pare că Pavel Vrublevski și-a creat propria rețea de farmacii ilicite – Rx-Promotion – în colaborare cu un vechi prieten al său, Iuri „Hellman" Kabaienkov. Vrublevski neagă faptul că ar fi jucat un rol activ în afacerile Rx-Promotion, dar, potrivit e-mailurilor scurse de la ChronoPay, el s-a întâlnit cu Leo Kuvaiev de la Rx-Partners și cu partenerul său, Vladislav Hoholkov, pentru a discuta despre participarea lui Rx-Promotion la cartelul aflat încă în stadiu de proiect. În e-mailurile scurse, Vrublevski susține că ar fi refuzat să participe la cartel, dar a spus că Mailien, SpamIt și un alt program important, EvaPharmacy, fuseseră de acord cu reducerea prețurilor la medicamente și cu limitarea comisioanelor afiliaților la 40%.

Jurnalele de chat pe care anchetatorii ruși le-au obținut până la urmă din computerul lui Stupin indică faptul că respectivul cartel s-a străduit asiduu să atragă rețeaua EvaPharmacy. Mai jos dăm transcrierea unei conversații desfășurate pe chat între Stupin și reprezentanții lui EvaPharmacy (numiți „Bulker.biz"). Discuția lor a fost tradusă din rusă în engleză.

STUPIN: Nu-mi plac condițiile pe care le oferim spammerilor. Unii dintre ei cer 45%. Noi suferim din cauza prețurilor scăzute, plus că unii dintre ei vor să-i plătim după o săptămână. Vreau să pun lucrurile la punct și să-mi plătesc mie mai mult decât lor ;) Nu plătim pe nimeni mai devreme de două săptămâni. Din cauză că plățile de la Șaman și din insule (off-shore) întârzie, soldurile conturilor noastre sunt în scădere.* Nu vă cer nimic, ci doar spun că și voi puteți fixa un termen de plată de minimum două săptămâni, iar spammerii nu vor avea de ales, pentru că noi vom oferi condiții similare. De asemenea, cred că vouă vă va fi mai ușor să plătiți dacă există o perioadă de așteptare, nu dacă lipsește, deoarece, dacă spammerii cresc producția, trebuie să țineți prea mulți bani lichizi în bănci. Pe scurt, ideea mea utopică este să creăm un cartel pentru a reduce comisioanele spammerilor la 30–35%, cât este profitul programelor de afiliere occidentale.

BULKER.BIZ: Și noi plătim tot după două săptămâni. Îi excludem însă [de la această restricție] pe spammerii noștri cei mai buni. Voi i-ați obligat pe mulți dintre spammerii noștri să treacă la voi după ce ați scăzut prețurile. Prin urmare, n-avem altă variantă ;) O înțelegere între noi ar fi grozavă, dar, ca să dea rezultate, trebuie să-i cooptăm pe Mailien și pe alții. În caz contrar, spammerii vor continua să plece la ei. Sigur că 45% este pur și simplu scandalos! Partnerka câștigă de trei ori mai puțin din cauza asta!

STUPIN: Da, iar singurul argument invocat de cei care cer 45% este că atât plătește Eva ;)

BULKER.BIZ: Unii plătesc chiar 50% și omoară piața și mai mult. Vreau să vă spun că știu despre ce spammer vorbești.





* Numele „Șaman" din această conversație este o referire la pseudonimul lui Nikolai Victorovici Illin, expertul IT în vârstă de 43 de ani aflat în spatele firmei Gateline.net. Gateline a fost un procesator de carduri de credit pe care SpamIt, GlavMed, Rx-Promotion și alți parteneri îl apreciau, se pare, pentru capacitatea sa de a procesa tranzacții MasterCard. Stupin și Gusev îl considerau pe Șaman un partener-cheie, egal cu ei în afacerea respectivă.

N-are nicio perioadă de așteptare, dar asta nu înseamnă că ne costă în fiecare zi tot profitul.

STUPIN: Știu, mi-a povestit totul.

BULKER.BIZ: Uite ce-i, suntem dispuși să ajungem la un acord și să stabilim aceleași condiții cu spammerii, dar numai după ce vom încerca niște furnizori noi și vom putea să reducem prețurile la un nivel cât mai apropiat de al vostru, numai când condițiile noastre competitive vor fi asemănătoare.

Potrivit lui Vișnevski, care a jucat un rol activ în crearea botnetului Cutwail, concluziile cercetătorilor UCSD, care arată că un număr mic de afiliați generează majoritatea veniturilor obținute de programele *partnerka,* sunt corecte. Vișnevski a spus că foarte puțini afiliați care nu dețin deja resurse semnificative de spam se pot aștepta să câștige mult din cauza costurilor mari pe care le presupune crearea lor.

Cea mai costisitoare parte a oricărei afaceri de spam este procesul de procurare a boților utilizați pentru a transmite e-mailuri nesolicitate. Aproape fără excepție, afiliații cu câștigurile cele mai mari au avut propriile botneturi, pe care le foloseau pentru a difuza propriul spam și care erau închiriate altor afiliați.

Vișnevski spunea că afiliații care folosesc resurse botnet de la alți spammeri o fac adeseori achiziționând „instalări", adică introducând într-un număr predefinit de boți un malware suplimentar care trimite spam pentru afiliat. Cei care închiriază boți de la alți afiliați plătesc adesea pentru că folosesc resursele respective redirecționând pur și simplu o cotă din comisioanele primite pentru fiecare vânzare realizată pe baza spamului generat de boții închiriați. Foarte des, spunea Vișnevski, botmasterii cer până la 50% din comisioanele unui client afiliat.

O rețea adecvată de spam nu constă însă doar în boți. Dacă am face o analogie între o rețea de spam și o fabrică, atunci boții ar fi utilajele responsabile de asamblarea părților

componente ale produsului finit. În plus, un botnet de spam este eficient doar în măsura în care softwareul care dirijează activităţile zilnice ale maşinăriilor este eficient. PC-urile moderne sunt foarte puternice, dar se pot bloca repede dacă li se cer simultan prea multe operaţiuni. Un software de spam satisfăcător distribuie volumul de lucru pe mii de PC-uri infectate în aşa fel încât fiecare computer să nu fie suprasolicitat.

În acelaşi timp, un software de spam bun ţine evidenţa numărului de e-mailuri livrate cu succes şi a numărului de destinatari care au accesat siteul promovat. Programul trebuie de asemenea să şteargă automat („scrub" în termeni tehnici) din listele de spam adresele de e-mail care nu mai sunt active sau care resping e-mailurile primite. Spammerii falsifică („spoof") frecvent adresa din secţiunea „from:..." a e-mailului nesolicitat, astfel că, atunci când mesajele spam sunt trimise unor conturi inactive, ele nu se întorc la spammeri, ci ajung la persoana neavizată a cărei adresă de e-mail a fost utilizată pentru a falsifica originea e-mailului! (Fără îndoială că aţi primit astfel de mesaje de la un prieten, un coleg sau o rudă al cărei cont de e-mail a fost spart sau falsificat.) E-mailurile care ricoşează astfel îi determină pe utilizatorii derutaţi şi îngrijoraţi ai internetului să se plângă furnizorilor de internet sau e-mail, care, la rândul lor, pot lua măsuri mai stricte de blocare a unor asemenea mesaje pe viitor.

În fine, un afiliat care nu are deja liste de adrese de e-mail valabile va trebui să le cumpere dacă nu-şi poate scrie propriul program care să obţină continuu adrese noi de e-mail de pe siteuri aleatorii.

Potrivit lui Vişnevski, un afiliat poate să cheltuiască 20–30% din totalul veniturilor cu închirierea de software şi liste de e-mail.

„N-ar trebui să ne surprindă faptul că majoritatea spammerilor nu câştigă prea mult dacă trebuie să închirieze toate aceste lucruri", a spus el.

Este imposibil de precizat cât cheltuiesc organizațiile din toată lumea cu combaterea e-mailurilor nesolicitate trimise de afiliați precum cei ai Rx-Promotion, GlavMed și SpamIt, dar este aproape sigur că mult mai mult decât ceea ce câștigă administratorii și fondatorii acestor programe.

Uluitor este faptul că, atunci când au calculat costurile directe și indirecte ale acestor programe în decurs de 11 luni, între mai 2009 și aprilie 2010, cercetătorii de la UCSD au constatat că profitul lor net reprezenta aproximativ 20% din venitul brut.

„Fascinant în toată treaba asta e că, trăgând linie, nu putem vorbi despre foarte mulți bani, a spus Savage de la UCSD. Deși indivizii care derulează asemenea programe nu sunt Donald Trump, activitatea lor are un impact financiar real și substanțial asupra vieții cotidiene a zeci de milioane de oameni. Cu alte cuvinte, pentru ca aceștia să câștige puțin, avem nevoie de o industrie de securitate de miliarde de dolari care să se ocupe de ei."

Savage și echipa lui de cercetători au avut, de asemenea, șansa să examineze multe dintre discuțiile purtate pe chat între Gusev și partenerul său de afaceri, Stupin. Acestea abundau în exemple legate de felul în care cei doi căutau permanent modalități de a adăuga valoare ofertelor adresate consumatorilor. Indivizi ca administratorii lui SpamIt au reușit în afacerile lor deoarece au înțeles piața de bază: produse livrate discret, la prețuri accesibile – de la pornografie on-line la pastile pentru mărirea penisului – pe care mulți adulți s-ar fi sfiit să le cumpere altfel.

La un moment dat, din discuții reiese că Stupin și Gusev s-au gândit să utilizeze infrastructura de spam pentru a promova un produs mult mai discutabil: dispozitivele de mărire a penisului.

„A fost de departe conversația cea mai amuzantă dintre toate, își amintea Savage. În esență, Gusev discuta în contradictoriu cu Stupin dacă ar trebui sau nu să adauge dispozitive de mărire a penisului în magazinele lor on-line. Gusev

susţinea cu tărie această idee. «Da, zicea el, americanii vor cu adevărat să-şi adauge câţiva centimetri», dar Stupin nu era convins. Asta încerc eu să le explic oamenilor [în virtutea] tuturor cercetărilor efectuate asupra acestei bizare economii subterane. În principiu, indivizii care se ocupă de farmacii şi spam nu se consideră deloc infractori. După părerea mea, ei cred că vând produse de calitate unui public care le cere. Da, poate că le stau în cale nişte legi, dar acestea sunt instrumentele unei structuri de putere occidentale şi nişte absurdităţi mic-burgheze legate de proprietatea intelectuală. Numai legea îi poate împiedica să vândă."



Dacă Savage are dreptate – că *partnerka* reprezintă „criminalitatea informatică dezorganizată" – atunci rolul creării şi menţinerii ordinii în pofida acestui haos aparţine forumurilor dedicate criminalităţii informatice. Acestea sunt comunităţi on-line în care majoritatea spammerilor, escrocilor şi şarlatanilor se întâlnesc, fac tranzacţii, câştigă şi menţin o reputaţie „demnă de încredere" în lumea subterană.

Forumurile de criminalitate informatică servesc câtorva scopuri principale. În primul rând, oferă răufăcătorilor relativ necunoscuţi şi celor aflaţi la începutul carierei posibilitatea de a-şi crea o reputaţie de furnizor sau cumpărător credibil de servicii. Dacă aceşti începători doresc să pornească o afacere în domeniul criminalităţii informatice – cum ar fi un botnet de spam – dar nu dispun de cunoştinţele sau resursele necesare creării unei anumite componente a acesteia, ei pot achiziţiona pur şi simplu componentele sau informaţiile lipsă de la alţi membri, se pot adresa membrilor importanţi ai acestor forumuri sau pot viziona tutorialele care oferă indicaţii şi soluţii.

În acest fel, forumurile respective contribuie aproape întotdeauna la coborârea obstacolelor care blochează intrarea pe piaţă a unor potenţiali răufăcători informatici. Ele oferă, de asemenea, escrocilor cu diferite abilităţi un loc în care să-şi

comercializeze și să-și testeze serviciile și produsele și, la rândul lor, să cumpere de la alții bunuri și servicii obținute în mod ilicit.

Există forumuri dedicate vorbitorilor tuturor limbilor importante și tuturor activităților specifice criminalității informatice, dar majoritatea sunt fie în limba rusă, fie în limba engleză. De asemenea, cele mai multe au o structură similară – o pagină principală cu linkuri către forumuri secundare, dedicate unei game largi de specialități, cum ar fi: spam, fraude bancare on-line, planuri de „golire" a conturilor bancare, dezvoltarea de malware, furt de identitate, fraude cu carduri de credit, escrocherii bazate pe câștigarea încrederii și fraudă publicitară sau tehnici de manipulare frauduloasă a poziției unui site în rezultatele oferite de Google și de alte motoare de căutare pe internet.

Chiar și forumurile dedicate unei forme specifice de criminalitate informatică – de pildă spamul – tind să adopte aceeași structură de tip subforum. În 2011, cercetătorii de la University of California din Santa Barbara și de Universitatea Ruhr din Bochum (Germania) au dat publicității o analiză minuțioasă a botnetului Cutwail, intitulată „The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns". În cursul cercetărilor pe care le-au desfășurat, aceștia au obținut baza de date cu acces indirect a forumului Spamdot.biz, acum dispărut – o comunitate infracțională informatică foarte strictă în privința securității. Ei au acceptat până la urmă să-mi pună la dispoziție, pentru documentare, toate informațiile siteului respectiv. În 2007, Spamdot a intrat în proprietatea lui Igor Gusev și Dmitri Stupin, administratori ai parteneriatelor farmaceutice GlavMed și SpamIt.

Din acest material a reieșit în mod limpede că, deși printre membrii săi se numărau unii dintre cei mai cunoscuți și performanți spammeri din lume, Spamdot a avut și zeci de membri a căror specialitate principală era să ofere servicii auxiliare din domeniul criminalității informatice, de la găzduire

web bulletproof şi înregistrare în masă a numelor de domenii până la vânzarea de liste de spam e-mail şi software care să-i ajute pe spammeri să şteargă din listele lor adresele invalide şi pe cele utilizate de activiştii antispam şi firmele de securitate.

Aceşti activişti împânzesc adesea internetul cu adrese de e-mail false în speranţa că spammerii le vor găsi şi vor expedia acolo spam. Atât ei, cât şi firmele de securitate folosesc spamul trimis la adresele false pentru a strânge informaţii despre cele mai recente malwareuri sau escrocherii de phishing propagate prin e-mailuri nesolicitate. Acestea ajută la estimarea dimensiunii şi locaţiei principalelor botneturi de spam, pe baza cărora antispammerii pot îmbunătăţi în general performanţa filtrelor de spam. Dar întrucât astfel de activităţi tind să reducă profitabilitatea şi stabilitatea oricărei operaţiuni de spam, spammerii cu experienţă recunosc importanţa pe termen lung a ştergerii adreselor false din listele de distribuţie. Este un joc constant de-a şoarecele şi pisica.



Subforumurile tind să fie moderate de escroci informatici consacraţi, care sunt experţi în domeniul lor. Nu este un fapt neobişnuit ca un infractor informatic să joace rolul de moderator al aceluiaşi subforum în mai multe forumuri distincte de criminalitate informatică. De exemplu, un escroc rus cunoscut sub pseudonimul „Severa" este sau a fost moderator al subforumului de spam în cel puţin patru forumuri importante de criminalitate informatică, inclusiv Spamdot. Aşa cum se va vedea în capitolul 7 („Să-i cunoaştem pe spammeri"), Severa este autorul unora dintre cele mai prolifice şi „de succes" botneturi de spam create vreodată. Ca atare, el cunoaşte practic toate numele importante din industria spamului şi deţine cunoştinţe vaste despre acest subiect, ceea ce îl face ideal pentru moderarea forumurilor de discuţii dedicate spamului.

Cei precum Severa sunt „liantul" viu care ţine laolaltă aceste comunităţi ale criminalităţii informatice. Ei posedă o mulţime de cunoştinţe despre domeniul lor şi se pricep să-i

pună pe novici în legătură cu membri mai experimentați, care caută parteneri sau subcontractori. De aceea, infractori ca Severa sunt ținte preferate ale autorităților, întrucât înlăturarea lor poate destabiliza deseori comunitatea infractorilor.

Multe forumuri de acest gen – în special cele nou-apărute – îi acceptă pe toți doritorii. Pe de altă parte, forumurile populate de unii dintre cei mai experimentați escroci informatici, care au cele mai multe relații, ridică diverse obstacole în calea membrilor noi, menite să-i separe pe hackerii utili și talentați de paraziți sau, mai rău, de posibilii reprezentanți ai autorităților care încearcă să se infiltreze și să culeagă dovezi despre activitățile ilicite ale spammerilor. Pentru a crea aceste măsuri de protecție, majoritatea forumurilor dedicate infractorilor informatici le cer solicitanților să menționeze cel puțin doi indivizi care sunt membri de încredere ai forumului și care pot da referințe sau „garanții", susținând că unul sau mai mulți membri ai forumului pot garanta abilitățile și integritatea solicitantului și l-au invitat să-și depună cererea de aderare.

În general, noii solicitanți trebuie să constituie un depozit nerambursabil, de obicei în monede digitale, cum ar fi WebMoney sau bitcoin. Presupunând că referințele confirmă faptul că membrii îl cunosc și pot garanta pentru abilitățile sale, solicitantului i se acordă acces limitat la forum, pe care îl poate folosi pentru a se prezenta comunității, pentru a-și pleda cauza și pentru a enumera lucrurile pe care le-ar putea face pentru forum dacă ar fi primit ca membru cu drepturi depline.

Membrii existenți pot folosi această perioadă de probă pentru a-l hărțui sau abuza verbal pe solicitant, pentru a-i testa cunoștințele de programare, hacking sau alte abilități legate de domeniul sau specialitatea sa. În felul acesta sunt eliminați novicii cei mai slabi. În cele din urmă însă, multe forumuri adoptă o atitudine democratică și lasă acceptarea definitivă a unui candidat în seama votului la care pot participa – dar nu sunt obligați să participe – toți membrii plini.

Ce anume îi determină pe oameni să participe la aceste forumuri şi de ce sunt atât de populare printre spammeri? Aşa cum un castel oferea în trecut locuitorilor săi protecţie împotriva atacatorilor şi tâlharilor, forumurile respective le oferă membrilor plini un minimum de protecţie (sau cel puţin un motiv de a face ceva) împotriva înşelăciunilor. Escrocii pot fi ei înşişi escrocaţi deoarece nu se pot adresa autorităţilor locale. La urma urmelor, tranzacţiile pe care le fac sunt, în majoritatea cazurilor, ilegale. Pentru a combate „înşelăciunile", forumurile impun un cod etic foarte strict, astfel încât membrii prinşi că încearcă să-şi trişeze colegii sunt ostracizaţi sau excluşi.

În primul rând, forumurile cele mai cunoscute oferă un serviciu de garanţie – reprezentând un mic procent din costul tranzacţiei – care reţine fondurile cumpărătorului până când acesta este mulţumit că vânzătorul şi-a respectat partea sa de înţelegere. Membrii vechi ai forumurilor insistă asupra utilizării garanţiei pentru toate tranzacţiile, în timp ce membrii mai zgârciţi şi mai puţin experimentaţi evită acest lucru pe propria piele.

Aşa cum casa de licitaţii on-line eBay îi încurajează pe utilizatori să-şi exprime părerile cu privire la calitatea tranzacţiilor pe care le-au desfăşurat cu alţi utilizatori, statutul membrului unui forum de escrocherii este determinat în parte de numărul punctelor de reputaţie („rep") pe care le-a acumulat în perioada petrecută pe forum. Membrii pot câştiga puncte pur şi simplu în urma participării regulate la firele de discuţii de pe diverse forumuri – în esenţă, împărtăşind celorlalţi cunoştinţele şi experienţa legată de criminalitatea informatică. Punctele sunt acordate sau retrase de membri consacraţi şi de moderatori ai forumului care au dobândit acest drept.

Sistemul este extraordinar de eficient în ceea ce priveşte reglementarea diferendelor dintre infractori. Aleksei Mihailov, expert rus în securitatea informaţiilor, care a examinat în mod exhaustiv documentele, conversaţiile de pe chat şi

alte materiale sustrase de pe forumul Spamdot, spunea că amenințarea unei singure postări negative pe forum îi determină pe acești indivizi să rezolve pe cale amiabilă diferende de zeci de mii de dolari. Accesul la forum și „poziția" lor în cadrul acestuia îi preocupă pe toți. Fără protecția și responsabilizarea specifice acestor refugii ale infractorilor, spammerii, escrocii și alți răufăcători on-line se confruntă cu un risc mult mai mare de a fi jefuiți de cei asemenea lor.

Membrii considerați de administratorii forumului ca făcându-se vinovați de multiple sau grave încălcări ale regulilor forumului pot primi rangul de „deer" (cerb) sau chiar eticheta mai serioasă de „ripper" (spintecător). „Deer" indică de obicei un membru nou care a încălcat regulile forumului în mod accidental sau pentru că nu este încă suficient de familiarizat cu ele. În general, cei etichetați astfel sunt considerați novici neștiutori, iar statutul lor îi avertizează pe alți membri ai forumului care lucrează cu ei că ar putea avea mai multe probleme decât în mod normal.

„Ripper" sunt cei dovediți a fi „escrocat" pe cineva prin neefectuarea unei tranzacții convenite anterior – fie prin refuzul de a plăti un serviciu sau produs, fie prin nelivrarea lor conform promisiunilor făcute. Partea vătămată trebuie să demonstreze administratorilor forumului că a fost escrocat, de obicei începând un fir de discuție într-un subforum numit „blacklist" (listă neagră). De cele mai multe ori, aceasta implică postarea unor lungi conversații anterioare care demonstrează presupusa infracțiune. Interesant este că ele pot fi adesea dovezi și informații de neprețuit pentru autoritățile și cercetătorii din domeniul securității, care acționează frecvent sub acoperire pe forumurile de criminalitate subterană.

Deși un forum mediu din domeniul criminalității are mulți membri – uneori zeci de mii – majoritatea celor mai active există pentru a aduce câștiguri administratorilor, liderilor subforumurilor și celor care vând servicii sau soluții la cheie

pentru restul comunității. Vânzătorii cei mai mari plătesc pentru ca firele lor de vânzări să-și păstreze poziția (*sticky*), astfel încât reclamele pe care le fac să rămână în partea superioară a paginii subforumurilor respective, având astfel o probabilitate mult mai mare de a fi citite de cei care caută ajutor în acele domenii ale criminalității informatice. În funcție de forum, pozițiile respective se vând anual sau lunar și variază ca preț de la o sută de dolari la câteva mii de dolari pe lună.

În ultimii ani, numărul de noi forumuri de criminalitate informatică a crescut foarte mult, ilustrând creșterea semnificativă a cererii de servicii ilegale și lupta acerbă care se dă între acestea pentru clienți. În timp ce multe comunități noi de infractori informatici dispar sau scad în importanță la scurt timp după apariție, altele sunt vechi de peste un deceniu, ceea ce indică faptul că industria criminalității informatice este foarte matură, fiecare piață având propriile mijloace de păstrare a ordinii, lucru în rețea și transfer rapid al informațiilor.





Încercările activiștilor antispam de a închide cele mai vechi comunități de infractori informatici – de obicei, prin exercitarea unor presiuni asupra furnizorilor de servicii de găzduire sau asupra firmelor care se ocupă cu rezervarea numelor de domenii, ori ambele – se întorc în cele din urmă împotriva lor. Forumurile își transferă pur și simplu domeniile la un alt furnizor de găzduire, mai blindat și mai bine protejat, care adoptă frecvent măsuri de securitate mai stricte, selectându-i cu mai multă atenție pe membrii noi și existenți, în căutarea unor semne care ar putea indica prezența autorităților și cercetătorilor sub acoperire.

Există însă o speranță: unele dintre inițiativele cele mai reușite de combatere a spamului și a epidemiei de malware s-au axat pe identificarea și capturarea celor mai mari spammeri din lume, ca și pe dezmembrarea mecanismelor utilizate de ei, așa cum vom vedea în capitolul următor și în capitolul 11.

# Capitolul 7

# SĂ-I CUNOAȘTEM PE SPAMMERI

Igor Vișnevski nu ar fi știut de unde sau cum să înceapă afacerea cu spam dacă n-ar fi existat legăturile pe care și le crease petrecând nenumărate ore pe câteva forumuri importante de criminalitate informatică de la vremea respectivă. La 19 ani, s-a înscris la o universitate din Moscova și visa să găsească un post de programator la o companie legală. A rămas însă destul de repede fără bani.

„Am studiat trei ani, după care părinții au încetat să-mi plătească facultatea pentru că nu mai aveau bani", a spus Vișnevski într-o discuție.

Puținele lucruri pe care le știa Vișnevski despre computere datau din adolescență, când părinții îi cumpăraseră un Sinclair ZX Spectrum, unul dintre primele PC-uri vândute în Europa. La început, Vișnevski a învățat singur diverse limbaje de programare, de la BASIC până la cele mai complexe. Ulterior, a achiziționat un PC la mâna a doua și a învățat PASCAL, un limbaj de programare conceput pentru elaborarea de software mai complex.

Tânărul și inteligentul hacker câștiga lunar între 200 și 300 de dolari, realizând siteuri pornografice pentru un program de afiliere administrat de Crutop.nu, creat de Vrublevski. Nu era însă nici pe departe suficient pentru a trăi la Moscova, așa că s-a angajat la o companie care vindea echipamente și servicii de încălzire și aer condiționat. Nici prin cap nu-i trecea că asta îl va duce în lumea spamului.

Într-o zi, șeful său i-a cerut ajutorul în promovarea serviciilor companiei prin mijloace mai puțin legale.

„La un moment dat, șeful a comandat prin spam de la cineva și mi-a spus că a fost grozav și că ar trebui să aflu cum să trimitem chiar noi spam, își amintea Vișnevski. Desigur, i-am spus că spamul era ceva rău, bla-bla, dar el mi-a zis că nu mai aveam comenzi și că trebuia s-o fac [pentru a atrage mai mulți clienți]."

Cercetarea întreprinsă de Vișnevski pentru șeful său în industria spamului l-a dus la Carderplanet.com, în acel moment, un foarte popular forum de limbă rusă în domeniul criminalității informatice. Carderplanet atrăsese mii de membri din toată lumea, care făceau schimb de informații pe diverse teme, de la administrarea botneturilor de spam la golirea conturilor bancare și de carduri de credit sparte.

Înființat în Ucraina în 2001, Carderplanet.com a fost grupul cel mai îndrăzneț de carderi (infractori care traficau carduri de credit furate), hackeri și hoți pe care l-a cunoscut vreodată internetul. Așa cum scrie Joe Menn în cartea sa intitulată *Fatal System Error*, în Ucraina nu exista practic o legislație privind pătrunderea neautorizată în sistemele informatice, așa încât grupul nu se temea să organizeze întâlniri publice și să facă publicitate serviciilor sale de hacking pe internet. Carderplanet avea să devină modelul după care au fost realizate aproape toate viitoarele forumuri din domeniul criminalității informatice, cu subforumuri pentru fiecare formă imaginabilă de specializare.

La Carderplanet, Vișnevski i-a fost prezentat lui Vardan Kușnir, un cunoscut spammer în vârstă de 35 de ani, care conducea American Language Center (ALC), o firmă de la Moscova care îi învăța limba engleză pe cetățenii ruși. Kușnir s-a oferit să-l ajute pe Vișnevski să înceapă o afacere cu spam dacă accepta, la rândul lui, să utilizeze o parte dintre resurse pentru a trimite e-mailuri nesolicitate destinate promovării serviciilor ALC.

„Mi-a oferit destui bani ca să închiriez servere și, în scurt timp, câștigam de patru ori mai mult decât la compania mea,

spunea Vișnevski. Am continuat totuși să lucrez acolo, fiindcă nu eram sigur că spamul reprezenta o sursă stabilă de venit. În două luni, devenisem deja destul de priceput la spam."

Datorită spamului trimis pentru mentorul său, Kușnir, Vișnevski a ajuns să facă cunoștință cu Dmitri „Gugle" Necivolod.

„Gugle era prieten cu Vardan și venea mereu la el ca să discute fel de fel de nimicuri, spunea Vișnevski. La un moment dat, am început și eu să comunic cu Gugle."

Adevărata afirmare a lui Vișnevski a venit însă după ce mentorul lui a fost ucis brusc, cu brutalitate. Într-o dimineață, mama lui Kușnir a găsit cadavrul însângerat al fiului ei în baie, cu capul crăpat. Conform unui articol din 2007 de pe Wired.com, operațiunea de spam a lui Kușnir trimitea zilnic peste 25 de milioane de mesaje nesolicitate, majoritatea promovând serviciile ALC și fiind expediate spre conturi de e-mail rusești. După părerea celor de la Wired.com și a lui Vișnevski, ignorarea flagrantă și repetată de către Kușnir a nemulțumirilor provocate de spam ar fi putut juca un rol esențial în asasinarea lui.

Netulburați de moartea lui Kușnir, Vișnevski și Gugle și-au unit resursele și au început propria afacere cu spam.

În octombrie 2011, am ajuns la concluzia că, în datele sustrase de la SpamIt și Rx-Promotion, existau suficiente informații pentru a trece la identificarea și schițarea profilului celor mai importanți spammeri din lume și, prin extensie, al celor responsabili de crearea și gestionarea celor mai mari botneturi de spam. Între numeroasele documente interne de la ChronoPay exista o foaie de calcul Excel intitulată banal „Date de înregistrare", care avea să devină cheia identificării multora dintre acești răufăcători.

Când am comparat datele respective cu alte informații despre câștiguri și date de contact pe care le aveam deja din documentele sustrase de la SpamIt, a reieșit limpede că, din motive necunoscute, cineva de la ChronoPay alcătuise această listă despre spammerii cei mai activi. Majoritatea spammerilor care lucrau pentru Rx-Promotion și SpamIt erau plătiți cu

WebMoney, care, așa cum am menționat, este o monedă virtuală, populară în Rusia și Europa de Est, utilizată pe scară largă în lumea hackerilor.

Conturile de WebMoney pot fi create sub pseudonim, pot fi configurate asemenea conturilor de card sau pot fi certificate în mod oficial. În ultimele două cazuri, solicitantul trebuie să prezinte o copie a pașaportului său la o unitate WebMoney autorizată înainte de a obține certificarea contului respectiv. Informațiile despre cont nu sunt făcute publice de WebMoney, dar se pare că un angajat de la ChronoPay a plătit pe cineva de la WebMoney ca să-i divulge numele și alte informații de contact legate de conturile utilizate de afiliații importanți din rețeaua SpamIt. A reieșit faptul că mulți dintre ei s-au ocupat de spam și pentru Rx-Promotion.

Dintre cele 163 de conturi WebMoney enumerate în listă, aproximativ o treime fuseseră certificate oficial sau erau conturi de card. Datele indicau identitatea WebMoney a afiliatului, numele, adresa, numărul de telefon, data nașterii, adresa de e-mail, numărul pașaportului și adresa oficială a instituției care eliberase pașaportul.

Multe dintre aceste conturi WebMoney fuseseră create cu mulți ani înainte ca proprietarii lor să înceapă să se ocupe de spam sau să participe la orice altă activitate infracțională informatică. Unul mi-a atras însă atenția într-un mod aparte. Între conturile certificate din lista respectivă exista un portofel WebMoney creat în ianuarie 2002 pentru un utilizator care folosise pseudonimul „Vânzător de software". Acest cont fusese creditat cu peste 175 000 de dolari pentru promovarea unor siteuri farmaceutice în numele SpamIt. De acolo aveam să încep.



## GUGLE

Timp de mai multe săptămâni, am studiat nenumărate convorbiri de chat desfășurate între acest utilizator – care

folosea pseudonimul „Gugle" atât în chatul de mesagerie instantanee ICQ, cât și pe Spamdot.biz – și administratorii parteneriatului farmaceutic SpamIt. În cele din urmă, am reușit să stabilesc faptul că era aceeași persoană care administra botnetul Cutwail, de departe cel mai mare și mai activ botnet de spam din acel moment. (Și în prezent este foarte activ.)

Lângă ID-ul corespunzător botmasterului Gugle, în listă apărea numele lui Dmitri Sergheevici Necivolod, născut la 9 iulie 1983 și domiciliat în Moscova. Când am văzut informațiile despre Necivolod, mi-am amintit o conversație purtată cu Vrublevski ceva mai devreme în acel an. Pe atunci nu-mi dădusem seama de importanța ei, pentru că nu cunoșteam rolul lui Gugle.

Spre sfârșitul anului 2010, Vrublevski mă sunase și-mi comunicase entuziasmat niște informații aflate de la contactele pe care le avea în rândul autorităților. Fusese anunțat că anchetatori în domeniul criminalității informatice de la NASA veniseră la Moscova pentru a se întâlni cu agenții FSB. Reprezentanții NASA, care au pistoale și insigne, și aceeași autoritate ca reprezentanții altor agenții americane de aplicare a legii, sosiseră pentru a discuta despre cooperarea cu autoritățile ruse în vederea anchetării lui Necivolod.

La vremea respectivă, anchetatorii de la NASA făcuseră legătura între Necivolod și Gugle, întocmindu-i celui dintâi dosar penal pentru presupusa infectare a nenumărate computere NASA cu malwareul Cutwail.

„Americanii au venit la Moscova încercând să-l găsească pe proprietarul Cutwail, care are pseudonimul «Gugle»", îmi spusese Vrublevski emoționat și cu mândrie la telefon, vorbind despre un individ care se numărase printre primii spammeri atât pentru Rx-Promotion, cât și pentru SpamIt. „I-au aflat pseudonimul și chiar numele adevărat, dar n-au reușit niciodată să-l prindă. Cred că l-a avertizat cineva. Știi, Brian, corupția în rândul autorităților rusești care se ocupă de criminalitatea informatică este foarte mare."

Nu sunt sigur nici acum de ce mi-a spus toate astea. Poate pentru a se lăuda că avea atât de multe relații în rândul autorităților, încât ar fi putut aranja ca unul dintre cei mai buni spammeri ai Rx-Promotion să nu fie predat agenților federali americani. Cred că dorea de asemenea ca anchetatorii NASA să știe că-i trăgea pe sfoară. La urma urmelor, aceiași anchetatori NASA convinseseră Comisia Federală pentru Comerț din SUA să-l deconecteze de la internet pe furnizorul de găzduire bulletproof 3FN, ceea ce provocase multe probleme și cheltuieli lui Vrublevski și rețelei lui de webmasteri de pornografie extremă și vânzători de antiviruși falși și spam.

Potrivit unei surse care a ajutat la desfășurarea anchetei NASA, Vrublevski fusese anunțat din timp de vizita americanilor de către agenți FSB corupți. Cu câteva zile înainte de întâlnirea programată dintre NASA și FSB, Necivolod a fugit din Rusia în Ucraina.





„Gugle și Pavel erau parteneri de afaceri și prieteni, a declarat sursa mea de la NASA sub protecția anonimatului, deoarece nu era autorizată să discute despre caz. Pavel a fost cel care i-a spus lui Gugle că [cei de la NASA] se întâlneau cu FSB ca să vorbească despre Cutwail. Se pare că, acum, Gugle se află în Ucraina, unde se ascunde."

Potrivit siteului firmei rusești de software Digital Infinity Developers Group, Necivolod făcea parte dintr-o echipă de programatori de elită care puteau executa diverse proiecte la diginf.ru. Pe pagina Diginf Team de pe siteul respectiv (acum inexistent), Dmitri Necivolod apărea ca „administrator de sisteme bazate pe UNIX", „administrator de routere Cisco" și „specialist în software de securitatea informațiilor". Ținând seama de experiența lui Nechvolod și a echipei sale de programatori, este clar că ei puteau sparge aproape orice sistem de comunicații sau de securitate.

Grupul lui Necivolod a păstrat o versiune de bază a codului botului Cutwail și a închiriat-o altor răufăcători pe forumuri

subterane, unde sistemul de spam era cunoscut sub denumirea de „0bulk Psyche Evolution".

În multe privințe, Necivolod este modelul infractorului cibernetic modern, o ocupație care se aseamănă cu aceea a traficantului de droguri prin faptul că generează un venit constant. Acești bani câștigați ilegal trebuie să fie ori spălați, investindu-i în proprietăți sau alte active, ori cheltuiți. Ca mulți dintre colegii săi, Necivolod a preferat să trăiască într-un ritm alert, înconjurat de lux, automobile rapide, fete ușoare, haine scumpe și droguri, spunea Vișnevski.

„Întotdeauna se îmbrăca foarte elegant, iar când și-a distrus limuzina Lexus de 100 000 de dolari, și-a cumpărat imediat un BMW", a spus acesta.

În 2008, afacerea cu spam a lui Necivolod înflorea. Botnetul Cutwail ajunsese la peste 125 000 de computere infectate și reușea să expedieze zilnic 16 miliarde de mesaje spam. În scurt timp, creșterea companiei l-a obligat să caute și să angajeze câțiva programatori noi. Pentru a ne face o idee despre ceea ce căuta, am reprodus mai jos un anunț pe care l-a postat pe Crutop.nu în tentativa de a găsi un programator talentat cu experiență în crearea de aplicații web.

> Tipul locului de muncă: birou local în Moscova (pachet de beneficii inclus), normă întreagă (9 ore pe zi, 5 zile pe săptămână).
>
> CERINȚE:
> • Cunoștințe excelente de Perl și PHP
> • Cunoștințe excelente de SQL
> • Cunoștințe de AJAX, JavaScript
> • Capacitatea de a scrie rapid coduri fără buguri
> • Vârsta minimă 22 de ani
> • Responsabilitate
>
> Salariul pentru perioada de probă 1 500 $ (1 lună), după aceea cel puțin 2 000 $.

Salariu pentru normă întreagă – cu beneficii – și posibilități de avansare. Ce și-ar putea dori mai mult un programator

tânăr și întreprinzător? Iar dacă 2 000 de dolari pe lună însemna un salariu foarte bun pentru un programator aflat la început care locuia în Moscova, era un vis pentru programatorii din provincie, care și-ar fi putut convinge șeful să-i lase să lucreze de acasă. Oferta lui Necivolod este încă o ilustrare a faptului că afacerile din domeniul criminalității informatice din unele părți ale lumii sunt în concurență directă cu multe companii legale aflate în căutarea programatorilor talentați.



## COSMA

Informațiile sustrase de la GlavMed–SpamIt și Rx-Promotion arată că unul dintre spammerii cei mai performanți ai ambelor parteneriate a fost un hacker care a folosit diverse pseudonime, printre care „Cosma", „Tarelka", „Bird" și „Adv1". Cosma, așa cum îl voi numi în continuare, și toate conturile sale afiliate SpamIt au câștigat peste 3 milioane de dolari sub formă de comisioane pe parcursul a trei ani de colaborare cu programul farmaceutic.

Mașina lui de spam a fost botnetul Rustock, o tulpină de malware lansată pentru prima dată pe internet în 2006. Numele botnetului era inspirat de scopul său inițial, acela de a comite o formă de fraudă în domeniul valorilor imobiliare cunoscută sub numele de *pump-and-dump* (umflă-și-aruncă). Escrocii cumpără foarte multe acțiuni la un preț mic de la companii cu o valoare de piață foarte mică (prețul unei acțiuni variază, de obicei, între mai puțin de un penny și câțiva cenți), expediază milioane de e-mailuri nesolicitate care prezintă acțiunile respective ca pe o șansă ce nu trebuie ratată, după care vând acțiunile imediat ce prețul lor crește din cauza naivilor care au fost păcăliți și au cumpărat.

În 2007, cercetătorii au început să observe că PC-urile infectate cu Rustock distribuiau și spam farmaceutic. Experții de la Dell SecureWorks au estimat, cam în aceeași perioadă, că Rustock infectase peste 150 000 de PC-uri și era capabil să răspândească zilnic până la 30 de miliarde de mesaje nesolicitate.

Apariția spamului farmaceutic de la Rustock coincide cu momentul în care Cosma devine afiliat la SpamIt. Cele trei nume pe care botmasterul lui Rustock le folosea în relația cu SpamIt – Cosma2k, Bird și Adv1 – au fost folosite pentru contul ICQ de la Rx-Promotion, gestionată de Vrublevski. Datele sustrase de la ChronoPay arată că aceste trei conturi au câștigat împreună aproximativ 200 000 de dolari sub formă de comisioane, promovând siteuri farmaceutice pentru Rx-Promotion în 2010.

În câteva conversații, Cosma se întreabă ce ar trebui să facă cu zeci de mii de PC-uri compromise, dar altfel inactive, aflate sub controlul său. Din toate discuțiile dintre Stupin și Cosma reiese clar că acesta din urmă avea acces la resurse interne SpamIt pe care alți spammeri nu-l aveau și că juca un rol oarecare în conducerea afacerii.

Într-o conversație datată 14 octombrie 2008, Cosma i-a spus lui Stupin că era hotărât să facă mai mulți pași înapoi după ce atrăsese atenția altor răufăcători, ceea ce nu era de dorit. Potrivit afirmațiilor sale, fusese răpit și ținut ostatic de niște golani care puseseră ochii pe el din cauza ultimului model de Porsche Cayenne, o mașină sport care costă cu mult peste 100 000 de dolari la Moscova. După ce fusese bătut de răpitori, Cosma le dăduse cheile mașinii. El i-a spus lui Stupin că, în urma incidentului, a hotărât să înlocuiască mașina furată cu un BMW 530xi mai puțin bătător la ochi.

Cosma a lăsat în urmă o serie de indicii despre identitatea sa reală. S-a înregistrat în programul SpamIt folosind adresa de e-mail ger-mes@ger-mes.ru. Siteul respectiv a dispărut în 2010, însă o copie a sa rămasă în memoria cache

arată că pagina de pornire conținea informații foarte interesante. Printre ele se număra CV-ul unui programator format în Belarus, care avea deasupra fotografia unui tânăr cu păr șaten, cu o cană de cafea în mână. Deasupra imaginii era numele: „Sergheev, Dmitri A." În partea de sus a paginii apărea un mesaj simplu: „Vreau să lucrez la Google." Sub CV se afla adresa de e-mail a autorului, urmată de mesajul: „Vă aștept oferta!"

Dacă golanii care i-au furat mașina lui Cosma știau cine este, aceștia l-ar fi putut preda celor de la Microsoft. În iulie 2011, Microsoft a oferit o recompensă de 250 000 de dolari pentru informații care puteau duce la arestarea și condamnarea botmasterului lui Rustock. Cosma rămâne în libertate.



## SEVERA

Cosma și-a administrat afacerea de spam în tandem cu cea a altui infractor informatic, hackerul cu pseudonimul „Severa". În 2007, acesta a fost inculpat într-un caz judecat de un tribunal federal din SUA, în calitate de partener principal al spammerului american Alan Ralsky, condamnat în 2009 fiindcă îi plătise pe Severa și alți spammeri pentru a promova escrocherii de tipul *pump-and-dump*. Deși a fost acuzat, Severa nu a fost arestat niciodată, iar cazul lui așteaptă să fie rezolvat. Acest lucru se datorează parțial faptului că el pare să se afle tot în Rusia, o țară care, în mod tradițional, n-a extrădat presupuși infractori informatici pentru a fi judecați în SUA sau în Europa.

Mașina de spam a lui Severa funcționa datorită unui vierme informatic sofisticat, cunoscut sub numele de „Waledac", care a apărut în aprilie 2008, deși mulți experți cred că acesta nu era decât o actualizare a viermelui Storm, motorul din spatele unui botnet de spam masiv care apăruse în 2007.

Waledac și Storm au fost principalii distribuitori de spam farmaceutic și malware. La apogeul său, Waledac a fost responsabil de expedierea zilnică a 1,5 miliarde de e-mailuri nesolicitate. Potrivit celor de la Microsoft, într-o singură lună, aproximativ 651 de milioane de e-mailuri nesolicitate care puteau fi atribuite lui Waledac au fost direcționate către conturi Hotmail, incluzând oferte și escrocherii legate de farmacii on-line, imitații de produse, locuri de muncă, acțiuni cotate în cenți și multe altele. Viermele Storm a difuzat de asemenea miliarde de mesaje zilnic și a infectat aproximativ un milion de computere din toată lumea.

Atât Waledac, cât și Storm erau foarte originali, deoarece dețineau mecanisme de autoapărare proiectate special pentru a-i împiedica pe cercetătorii din domeniul securității să-i dezasambleze. Botneturile tradiționale sunt controlate de servere de internet care pot fi închise, așa cum s-a întâmplat cu McColo sau Atrivo. Waledac și Storm trimiteau însă actualizări și alte instrucțiuni prin intermediul unui sistem de comunicații *peer-to-peer* similar cunoscutelor servicii de partajare de muzică și fișiere. Frumusețea acestei metode consta în aceea că, chiar dacă cercetătorii din domeniul securității sau autoritățile reușeau să pătrundă în serverele de control indirect ale botnetului și să cureță un număr uriaș de PC-uri infectate, botneturile se puteau multiplica ele însele prin transmiterea de actualizări de software de la un PC infectat la altul.

Potrivit datelor de la SpamIt, Severa a adus venituri totale de 438 000 de dolari și a câștigat 145 000 de dolari sub formă de comisioane pentru expedierea de publicitate în favoarea unor siteuri farmaceutice ilicite într-o perioadă de trei ani. A fost, de asemenea, unul dintre moderatorii de pe Spamdot.biz.

Severa a câștigat mai mult din închirierea botnetului său altor spammeri. Pentru 200 de dolari, utilizatorii verificați îi puteau folosi botnetul pentru a trimite un milion de spamuri.

Campaniile de e-mail nesolicitat care promovează oferte de serviciu sau escrocherii de tipul *money mule* costă 300 de dolari milionul de mesaje, iar e-mailurile de phishing puteau fi expediate prin botnetul lui Severa pentru 500 de dolari milionul de mesaje.

În conversațiile de chat sustrase de la SpamIt există dovezi ample că Severa a controlat botnetul de spam Waledac. Pe 27 august 2009, el a trimis un mesaj privat unui utilizator Spamdot.biz numit „IP-server". Informațiile arată că acesta din urmă i-a oferit lui Severa acces contra cost la servicii de „găzduire bulletproof" care aveau să reziste acuzațiilor repetate de abuz din partea altor furnizori de servicii de internet (ISP). Mesajele arată că Severa a negociat cu IP-server achiziția de servere dedicate, folosite pentru controlul operațiilor botnetului Waledac.



În mesajul său, Severa i-a scris lui IP-server (traducere din limba rusă): „Salut, scriu pe contul tău ICQ, nu răspunzi. Un server a căzut timp de 5 ore. Cel care se termină în .171. Care-i problema, revine sau nu, și când?" Severa a atașat apoi mesajul de eroare transmis de serverul cu probleme. IP-server trebuie să fi rezolvat deficiența, deoarece adresa de internet despre care se plângea Severa – 193.27.246.171 – avea să fie detectată după o zi de analiștii malware și etichetată ca server de control pentru botnetul Waledac.

În actul federal de acuzare, numele lui Severa apare ca „Peter Severa", dar numele de familie poate fi fals. Potrivit activiștilor antispam de la Spamhaus.org, numele real al lui Severa este Piotr Levașov.*

* L-am contactat pe Severa folosind adresa de mesagerie instantanee care apare pe mai multe forumuri de criminalitate informatică, pe care este moderator global pentru discuții despre serviciile de e-mail nesolicitat și spam. Persoana care a răspuns mesajelor trimise la adresa respectivă a spus că nu cunoaște niciun Severa, că nu a folosit niciodată botneturi pentru campanii de e-mail în masă și că

De ce ar trebui de fapt să-i pese cuiva de Severa? La fel ca în cazul asociatului său – Cosma, botmasterul lui Rustock – pentru capul lui Severa este posibil să existe o recompensă de 250 000 de dolari. Viermele Conficker, lansat în 2009, care a infectat cu repeziciune între 9 și 15 milioane de computere din toată lumea, a determinat o reacție internațională fără precedent din partea experților în securitate. Acest grup de experți, poreclit „Cabala Conficker", a încercat în zadar să limiteze răspândirea viermelui.

În ciuda infectării unui număr imens de computere care rulau Microsoft Windows, Conficker n-a fost totuși utilizat niciodată pentru spam. De fapt, PC-urile infectate cu Conficker nu au făcut decât să descarce și să distribuie o nouă versiune a botnetului Waledac. Ulterior, în același an, Microsoft a anunțat că oferă o recompensă de 250 000 de dolari pentru informații ce puteau duce la arestarea și condamnarea autorului sau autorilor lui Conficker. Unii experți în securitate consideră că acest lucru dovedește existența unei legături între Severa și Conficker.

Severa și Cosma s-au întâlnit de câteva ori în perioada în care au colaborat în afacerea cu spam pentru acțiuni și par să se fi cunoscut destul de bine pentru a se tutui. Informațiile care mi-au parvenit de la Spamdot.biz conțin mesaje private schimbate între ei la 25 și 26 mai 2010. În ele, Severa îi spune lui Cosma „Dimas", o formă familiară a lui „Dmitri". În mod similar, Cosma îi spune acestuia „Petka", un diminutiv rusesc comun al lui „Piotr".

Atât Severa, cât și Cosma continuă să fie liberi și destul de activi în domeniul spam și malware.* Severa este administratorul unor subforumuri de spam pe mai multe forumuri subterane, oferindu-și serviciile de spam la un preț cu mult

a desfășurat numai campanii de mică amploare, bine țintite, pentru clienții săi.

* Severa a fost extrădat în SUA de autoritățile spaniole în februarie 2018 (n. red.).

inferior majorității prețurilor pe care le practica în 2008. Botneturile de spam pe care le gestionează continuă să bombardeze conturile de e-mail cu mesaje nesolicitate prin care se promovează produse dubioase și se răspândește malware.

## GERA

Potrivit datelor sustrase de la SpamIt, al doilea afiliat ca importanță din program a fost cel cu pseudonimul „GeRa". Pe parcursul a trei ani, publicitatea făcută de GeRa și de cei recomandați de el a avut ca rezultat realizarea a cel puțin 80 000 de tranzacții cu produse farmaceutice contrafăcute, a adus rețelei SpamIt venituri de peste 6 milioane de dolari, iar lui și prietenilor lui, peste 2,7 milioane de dolari.

Multe date indică fatpul că GeRa este principalul hacker din spatele lui Grum, un botnet de spam care distribuia zilnic peste 18 miliarde de e-mailuri înainte de a fi închis în 2012.

GeRa și Stupin discutau prin chatul ICQ aproape zilnic, de obicei din cauză că GeRa se plângea că o parte a infrastructurii lui de spam nu funcționa corect. De fapt, Stupin susținea că GeRa era de departe cel mai sâcâitor dintre toți spammerii importanți ai programului, spunând unui coleg administrator din rețeaua SpamIt că „nici Docent [botmaster pentru Mega-D], nici Cosma [botmaster pentru Rustock] nu se pot compara cu el în privința problemelor create de furnizorii de hosting".

Câteva conversații ale lui Stupin arată că GeRa avea probleme cu anumite adrese de internet care, ulterior, aveau să fie semnalate ca servere de control pentru botnetul Grum. De exemplu, într-o discuție cu Stupin din 11 iunie 2008, GeRa a postat un link către adresa 206.51.234.136. Apoi, după ce a verificat serverul, i-a spus lui Stupin câte PC-uri infectate se conectau la acea adresă în momentul respectiv. Același server era de multă vreme considerat un controler pentru botnetul Grum.

Grum devenise deja un pericol atât de notoriu, încât a fost menționat în studiul „Top Spam Botnets Exposed", întocmit de Joe Stewart de la Dell SecureWorks. La 13 aprilie 2008, la numai cinci zile după publicarea analizei lui Stewart, GeRa avea să posteze un link spre ea într-o conversație pe chat cu Stupin, spunând: „Ha, ha, și eu sunt pe listă!"

Discuțiile dintre GeRa și Stupin arată că, la un moment dat, GeRa a părăsit SpamIt ca să colaboreze cu Rx-Promotion. Cercetătorii de la University of California din San Diego (UCSD) care au studiat datele obținute despre afiliații rețelei Rx-Promotion au remarcat că toate siteurile farmaceutice Rx-Promotion includeau în codul-sursă un „site_id", care identifica în mod unic farmacia pentru plata ulterioară a comisioanelor de publicitate. Cercetătorii au descoperit că, ori de câte ori Grum promova un site Rx-Promotion, identificatorul era 1811. Conform informațiilor din baza de date Rx-Promotion, ID-ul afiliat aparține utilizatorului „gera".

„Aceasta nu dovedește că GeRa deținea Grum, a spus profesorul Stefan Savage, membru al grupului pentru sisteme și rețele de la UCSD și coautor al studiului, ci arată că, atunci când Grum a făcut publicitate pentru Rx-Promotion, a fost vorba despre siteuri la care comisioanele erau plătite unei persoane cu pseudonimul GeRa."

În conformitate cu informațiile despre plăți scurse de la GlavMed și Rx-Promotion, GeRa a primit comisioane pentru toate aceste conturi în portofelul WebMoney cu numărul de identificare 112024718270. Potrivit unei surse care are capacitatea de a căuta informații despre identitate atașate conturilor WebMoney, portofelul a fost creat în 2006 de către o persoană care a prezentat un pașaport rusesc la un birou WebMoney de la Moscova. Numele de pe pașaport era Nikolai Alekseevici Kostogriz, iar persoana avea 26 de ani. (Nu am reușit să-l contactez pe Kostogriz pentru a confirma dacă GeRa era într-adevăr el sau dacă identitatea îi fusese furată.)

Informațiile despre discuțiile avute pe chat de Stupin și mesajele personale ale lui GeRa de pe Spamdot.biz ne prezintă un hacker agresiv, certăreț, care părea mereu supărat din cauză că era înșelat de cineva. GeRa avea un vechi conflict cu FTPFire, un membru al SpamIt recomandat de el. Într-una dintre conversațiile avute cu Stupin, GeRa a spus că ar fi vrut să pună mâna pe el și să-l „aranjeze" în „stil italian". I-a mai spus lui Stupin că avea pe statul de plată niște polițiști cărora le ceruse să localizeze FTPFire.

GeRa a mai afirmat că fusese jefuit de 30 000 de dolari când își încetase activitatea o *partnerka* de antiviruși iliciți cu care colabora. Compania respectivă, numită BakaSoftware, făcea afaceri ilicite cu scareware, bombardând victimele cu avertismente tot mai alarmante despre riscurile de securitate și virușii de pe PC-urile lor. Acele avertismente aveau să continue până când victima fie plătea licența pentru un software de securitate adeseori inutil, fie găsea o modalitate de a elimina programul invaziv.*

Deși nu este clar dacă GeRa mai activează în domeniul spam, contribuția lui în domeniul e-mailurilor nesolicitate dăinuie. Codul-sursă pentru botnetul Grum a fost vândut mai multor spammeri care se pare că l-au modificat pentru a corespunde propriilor scopuri și-l folosesc în prezent pentru răspândirea de e-mail nesolicitat.



## ENGEL

Puțini botmasteri au fost la fel de furioși și de răzbunători ca „Engel", pseudonimul spammerului rus condamnat Igor A. Artimovici și al fratelui său, Dmitri. Se pare că Engel a gestionat botnetul Festi și, o perioadă, a creat spam atât pentru

* Merită amintit faptul că procesatorul principal de carduri de credit al companiei BakaSoftware a fost ChronoPay.

Rx-Promotion, cât şi pentru SpamIt. În 2009 însă, o serie de incidente şi altercaţii produse între el şi administratorii SpamIt l-au întors pentru totdeauna împotriva programului SpamIt, făcându-l să devină un aliat de nădejde al lui Pavel Vrublevski. În mod paradoxal, acea alianţă avea să ducă într-un sfârşit la distrugerea lui Vrublevski şi a Rx-Promotion.*

Detectat prima dată în toamna anului 2009, Festi a devenit repede o ameninţare potenţială pe scena botneturilor. Potrivit celor de la ESET, o firmă slovacă de securitate şi antiviruşi, Festi era în acel moment unul dintre cele mai puternice şi mai active botneturi folosite pentru spam şi lansarea unor atacuri DDoS. Foarte activ şi, adesea, combativ pe forumul Spamdot.biz, Engel numea propriul botnet „Topol Mailer", referire indirectă la racheta balistică intercontinentală rusească Topol-M – un nume potrivit pentru un botnet care distribuia la un moment dat o treime din tot spamul spre conturi de e-mail din toată lumea, dar mai ales spre americani.

Profilul lui Engel de pe Spamdot.biz conţinea adresa de e-mail „support@id-search.org". Domeniul respectiv nu mai este on-line, însă cei de la archive.org arată că Engel a folosit-o ca bază pentru un bot al cărui singur scop era să strângă adrese de e-mail de pe miliarde de pagini web. Engel a susţinut public că botul n-a fost decât un proiect de cercetare, dar s-a lăudat în particular pe Spamdot că acesta putea examina simultan sute de siteuri şi putea alcătui rapid liste cu adrese de e-mail de „sute de megaocteţi".

La începutul colaborării cu SpamIt, Engel a bănuit că Gusev şi Stupin îi „bărbiereau" comisioanele – în esenţă, nu-i plăteau toţi banii la care avea dreptul în urma vânzărilor realizate pe siteuri farmaceutice pe care le promovase folosind spam

* Potrivit unui reportaj apărut în *New York Times* în 2013, Artimovici nu neagă folosirea pseudonimului Engel, dar respinge faptul că a folosit botneturi sau a distribuit spam şi spune că a fost angajat de ChronoPay numai pentru a ajuta compania să realizeze un antivirus.

difuzat de botnetul Festi. Gusev și Stupin au negat că îi bărbiereaucomisioanele–șiaveaudreptateînaceastăprivință–dar discuțiile private ale lui Stupin de pe chat arată că acest lucru era doar pe jumătate adevărat.

Conversațiile respective demonstrează că botmasterul lui Cutwail, Gugle (Dmitri Necivolod), deturnase cumva porțiuni din traficul lui Festi și deviase spamul destinat siteurilor farmaceutice promovate de Engel spre propriile farmacii on-line. Gusev și Stupin știau asta, dar nu păreau dispuși să ia măsuri – în special pentru că nu-l puteau suferi pe Engel și bănuiau deja că era foarte apropiat de Vrublevski.

În 2009, Engel a devenit atât de furios din cauză că era înșelat la bani, încât a început să folosească forumul Spamdot.biz pentru a-și promova agresiv noul forum și parteneriat farmaceutic, Spamplanet.net. Repede și fără osteneală, a reușit să ademenească câțiva botmasteri importanți, printre care și pe Cosma, botmasterul lui Rustock.



Gusev și Stupin au stabilit că această activitate, combinată cu afirmațiile publice tot mai vehemente ale lui Engel despre bărbierirea comisioanelor, era inacceptabilă și i-au interzis accesul pe forum. Când administratorii SpamIt au ignorat cererile lui Engel de a-i reactiva contul, Engel a folosit botnetul Festi pentru a lansa o serie de atacuri DDoS zdrobitoare împotriva SpamIt și rețelei sale de siteuri farmaceutice, afectând încasările tututor membrilor parteneriatului.

Spammerii prezentați în acest capitol au creat și au administrat unele dintre cele mai puternice și mai distrugătoare botneturi de spam din lume și, drept urmare, sunt ori au fost responsabili în foarte mare măsură de e-mailurile nesolicitate expediate zilnic la nivel mondial. Împreună, botneturile de spam au infectat, de-a lungul anilor, zeci de milioane de computere, timp în care au furat datele personale și financiare a nenumărați consumatori.

În mod individual, aceşti maeştri ai e-mailurilor nesolicitate au câştigat câteva milioane de dolari, obligând însă companiile şi consumatorii să cheltuiască sute de milioane de dolari pentru a se apăra zilnic de atacurile lor ilegale.

Aceşti spammeri au fost însă doar simpli vasali şi baroni aflaţi la conducerea fiefurilor care se războiau. Adevăraţii autori ai acestei asimetrii economice – liderii care au creat parteneriate farmaceutice – i-au folosit pe spammeri ca pe nişte pioni într-un joc de şah cu miză mare, un conflict costisitor căruia locuitorii lumii subterane digitale aveau să-i spună în curând „războiul farma".

## Capitolul 8

# PRIETENI VECHI, DUȘMANI ÎNVERȘUNAȚI



La începutul verii lui 2008, coproprietarul lui SpamIt, Igor „Desp" Gusev, pe atunci în vârstă de 27 de ani, își petrecea vacanța cu tânăra lui soție și fetița lor la Marbella, în sudul Spaniei, pe coasta pitorească a Mării Mediterane. Tocmai îi fusese oferit un post de funcționar public în Rusia, ca asistent în Ministerul Dezvoltării Economice, dar nu hotărâse deocamdată dacă să părăsească Spania și să accepte slujba respectivă.

În acel moment, SpamIt și GlavMed formau cea mai mare rețea de farmacii ilicite on-line de pe planetă și colaborau cu aproape toți spammerii importanți din lume. Ambele programe tocmai atinseseră nivelul maxim al câștigurilor, obținând un venit lunar de aproape 6 milioane de dolari.

În ciuda succesului, Gusev se gândea serios să accepte funcția guvernamentală și să renunțe la rolul de boss al lumii criminale informatice. Încă nu discutase cu partenerul său de afaceri, Dmitri Stupin, dar, la un moment dat, tot trebuia să-i spună. Cei doi creaseră GlavMed și SpamIt de la zero, transformându-le într-o afacere înfloritoare, dar, în ultima vreme, între ei apăruseră neînțelegeri. Gusev dorea să ducă o viață în limitele legii, stabilă, alături de familia sa. În același timp, pe Stupin îl nemulțumea tot mai mult faptul că partenerul său

călătorea întruna şi-l lăsa pe el să se ocupe de problemele zilnice ale conducerii unei afaceri care se baza în mare măsură pe infractori.

Următoarea discuţie dintre Gusev şi Stupin, care provine dintr-un jurnal de chat, a fost consemnată în vara anului 2008, a fost tradusă în limba engleză de Aleksei Mihailov şi ilustrează resentimentele care clocoteau în Stupin. Ea include de asemenea o temă existentă în multe dintre conversaţiile lor: Stupin se gândea mereu la modalităţi noi de a câştiga bani, pe când Gusev părea că-şi doreşte un trai mai decent, chiar dacă ba chiar mai banal.



GUSEV: Îmi place foarte mult în Spania :) Totuşi distracţia e umbrită de viitorul „job"; vom vedea ce naiba o mai fi şi asta.

STUPIN: Ce fel de „job"? Despre ce vorbeşti?

GUSEV: Am de gând să mă angajez la Ministerul Dezvoltării Economice, ca asistent al ministrului adjunct.

STUPIN: Hmm... ai decis până la urmă s-o faci? Dacă te gândeşti bine şi îţi investeşti timpul şi eforturile în ceea ce avem deja, putem creşte profiturile de două până la trei ori, ceea ce înseamnă câteva milioane de dolari în plus pe an doar pentru tine.

GUSEV: Aşa este, dacă vrei să câştigi bani :) E prea mult de explicat ca să o fac în scris. Hai să luăm prânzul la un moment dat la Moscova şi o să-ţi explic de ce vreau slujba asta. Iată însă şi versiunea scurtă: în ţara noastră, cel mai important nu este să câştigi bani. Cel mai important este să-i păstrezi, să-i înmulţeşti şi să te asiguri că nu-i va înhăţa altcineva. În prezent, sursa noastră principală de venit este o afacere semilegală. Dacă ei vor să ne termine, o pot face cât ai zice peşte. N-o să fie uşor să scap, chiar şi cu relaţiile pe care le am acum în politică. Scopul principal este să nu pierdem ceea ce avem deja şi să nu ne lăsăm doborâţi.

STUPIN: Dacă e vorba să nu pierzi, cumperi pur şi simplu proprietăţi imobiliare în străinătate. E o soluţie mai „mobilă"

decât crezi. Dacă se împute treaba, ne putem descurca şi cu patru–cinci persoane. Toţi ceilalţi sunt doar pentru dezvoltarea afacerii.

GUSEV: Nu vorbesc despre bani, ci despre afacere în sine. Dacă noi doi dăm de belea, s-a zis cu toată „mobilitatea" asta. Prin urmare, vreau să fac în aşa fel încât să nu le fie uşor să ne creeze probleme. Trebuie să recunoşti că afacerea nu va supravieţui fără noi doi. Andrei, Margo, Saşka, Stratos nu vor reuşi singuri.

STUPIN: În ultimul timp, am senzaţia că vorbesc singur. Te calc pe nervi?

GUSEV: Nu, de ce crezi asta?

STUPIN: Te porţi altfel. Nu mai există comunicare.

GUSEV: Şi eu am aceeaşi impresie. Scriu ceva şi nu primesc niciun răspuns. Din când în când, mai scrii „OK":)

STUPIN: Eu nu te mai consider un „muncitor", un om cu care colaborez. Comunic în mod constant cu Andrei şi cu Saşka. Discut totul cu ei. Fie eşti absent, fie nu faci nimic (aşa mi se pare). Asta nu mă calcă pe nervi, nu mă irită. Pur şi simplu, nu te mai consider o persoană cu care trebuie să colaborez sau cu care pot să colaborez.

GUSEV: În privinţa jobului, ai de multă vreme autoritate deplină. E mai eficient aşa.

STUPIN: Mie îmi convine mai degrabă să nu comunic prea mult cu tine, pentru că, în caz contrar, încep să mă întreb de ce avem de fapt nevoie de tine. Ar fi mai bine să începi să faci ceva, altfel voi continua să discut tot mai puţin cu tine.

GUSEV: Îţi mulţumesc pentru sinceritate, dar nu ţi-am oferit şansa de a ajunge partener din simplu programator doar pentru ca, la un moment dat, să-mi spui că nu mai sunt necesar. Ai fi fost un foarte bun programator la o companie importantă, cu un salariu de cinci până la şapte mii şi nu ţi-ai fi putut cumpăra casa din Turcia dacă nu ne-am fi întâlnit atunci şi dacă eu nu ţi-aş fi permis să te ocupi de firmă. Gândeşte-te bine la asta. Banii îi orbesc pe oameni şi le dau impresia falsă că deţin toată puterea.

STUPIN: Am spus eu că ai devenit inutil? Tu crezi asta. Dacă te-ai fi gândit niţel, ai fi înţeles că eu sunt motivul pentru care merge totul atât de uşor şi bine, doar pentru că am devenit cel care mi-ai dat voie să devin.

GUSEV: Să vorbim diseară. O să mă mai liniştesc.

STUPIN: Sigur că da. Eu n-am nicio problemă.

Disputa a fost suspendată însă din cauză că a apărut o problemă mai presantă. În timp ce se afla în sudul Spaniei, Gusev a primit un mesaj urgent de la un prieten numit Aleksei, un hacker care îi furniza informaţii privind interesul autorităţilor pentru activitatea spammerilor.



LEHA: Hei. Eşti acolo? Te-am căutat.

GUSEV: Scuze, am fost în Spania cu familia.

LEHA: A apărut o chestie nasoală pe care trebuie s-o ştii. Ascultă-mă şi după aceea trage singur concluziile.



Leha i-a explicat că, în urmă cu câteva seri, se întâlnise cu Iuri „Hellman" Kabaienkov, partenerul lui Vrublevski de la Rx-Promotion. Aşa cum se întâmpla adeseori, Kabaienkov era beat, iar, în seara aceea, Leha îl auzise lăudându-se că i-a mituit pe poliţişti ca să deschidă o anchetă penală împotriva afacerii lui Gusev.

LEHA: Din întâmplare, m-am întâlnit săptămâna trecută cu Hellman, care era beat. Iar acesta, fie ca să se laude, fie doar pentru că e un dobitoc, a spus tot. M-a întrebat: „Mai ţii legătura cu Desp (Gusev)?" A fost în mod clar o întrebare cu subînţeles. I-am zis imediat: „De ce întrebi?"

Hellman a dat de înţeles că „cei sănătoşi la minte" vor începe să se distanţeze de Gusev şi că a văzut el însuşi dosarul, în care se preciza că acesta urma să fie acuzat de spălare de bani.

GUSEV: Ce încearcă să-mi pună în cârcă?

LEHA: Articolul din codul penal care se referă la legalizarea veniturilor provenite din activităţi infracţionale. Nu ştiu dacă dosarul există sau nu cu adevărat, eu îţi spun doar ce

am auzit. Sunt șocat de o așa prostie. Evident, Pașa [Pavel Vrublevski] a început totul, dar faptul că Hellman s-a băgat în treaba asta e de-a dreptul ridicol.

GUSEV: Mulțumesc, Leha. M-ai avertizat la timp.

LEHA: Hellman voia să cumpere o mașină. Dacă mai ții minte, s-a lăudat cu asta la petrecerea de ziua mea... La un moment dat însă, a spus că trebuie să amâne achiziția fiindcă are nevoie de mulți bani pentru ceva. Iar acum, beat fiind, a lăsat să-i scape exact motivul pentru care are nevoie de bani.

GUSEV: Știi cumva ce procuratură instrumentează cazul?

LEHA: Nu știu nici procuratura, nici cine a inițiat cazul. Nici măcar nu sunt sigur că dosarul există. Eu nu l-am văzut.

GUSEV: Dar ce motiv ar avea Hellman să mă vadă anchetat penal? Ce i-am făcut?

LEHA: E o absurditate. N-am idee ce motiv ar putea avea. L-am întrebat și mi-a răspuns: „De ce să n-o fac?" Pașa [Vrublevski] e un nenorocit. Toată aiureala asta e prea din cale afară.

GUSEV: Ce mă amuză e că el încă îmi datorează bani.

LEHA: Numai gura e de el. Spune că generali și colonei din poliție lucrează pentru el. Hellman vorbește des despre porcăria ăsta. Spune că are totul sub control.

GUSEV: Dacă poți să afli ce procuratură instrumentează cazul, o să fie mult mai ușor să găsesc dosarul.

LEHA: Igor, am o presimțire foarte nasoală despre situația asta. Nu poți să rezolvi problema altfel?

GUSEV: Încep chiar acum să mă ocup de ea. Nu sunt 100% sigur, dar voi cere ajutorul unor oameni foarte serioși. Știi și tu, nici Dumnezeu nu garantează rezolvarea tuturor problemelor.

Așa a început războiul farma, un conflict de lungă durată, public și, în ultimă instanță, extrem de costisitor între proprietarii celor mai mari *partnerka* farmaceutice din lume în acel moment – un conflict care avea să schimbe pentru totdeauna cursul industriei spamului. Ancheta pe care se spune că Vrublevski și Hellman ar fi comandat-o împotriva lui Gusev și a

afacerii sale urma să declanşeze o serie de evenimente nefaste, cei doi întrecându-se în a cheltui din ce în ce mai mult pentru a mitui autorităţile şi a se distruge unul pe celălalt.

Amândoi aveau să reuşească.

Gusev crede că Vrublevski şi Hellman au plătit ca să se deschidă un dosar penal împotriva lui pentru că îl considerau întru câtva responsabil de o catastrofă financiară recentă, care provocase pierderi de peste 7 milioane de dolari uneia dintre afacerile lor. Banii pierduţi erau păstraţi drept garanţie pentru câţiva dintre cei mai buni hackeri ai Rusiei, iar consecinţele dispariţiei lor au făcut ca RedEye (Vrublevski) să devină rapid persona non grata printre webmasterii de pornografie şi spammeri.

Într-o discuţie telefonică, Gusev a spus că necazurile cu Vrublevski au început la scurt timp după ce acesta a fost victima unui raid corporativ care a dus la dispariţia câtorva milioane de dolari pe care se părea că Vrublevski îi datora webmasterilor ruşi de pornografie. Mulţi cititori occidentali sunt fără îndoială familiarizaţi cu conceptul de raid corporativ – cunoscut şi ca „preluare ostilă" – care presupune cumpărarea unui număr mare de acţiuni la o companie şi apoi utilizarea drepturilor de vot rezultate pentru a întreprinde schimbări, cum ar fi înlocuirea conducerii sau lichidarea companiei.

În Rusia însă, preluarea ostilă este de cele mai multe ori un eveniment violent, care se poate petrece fie cu ajutorul unor judecători sau politicieni mituiţi, fie sub ameninţarea armelor. Potrivit celor de la Knowledge@Wharton, o publicaţie a şcolii de afaceri Wharton, *70 000 de companii ruseşti sunt anual ţinta unor raiduri corporative.*

„La mijlocul anilor 1990, erau cât se poate de fireşti reportajele despre bărbaţi mascaţi şi înarmaţi cu automate Kalaşnikov, care năvăleau în sediile unor companii promiţătoare, confiscau active şi-i forţau pe proprietari să semneze documente de transfer de proprietate", scriau cei cinci membri ai promoţiei 2010 a Wharton's Lauder Institute care au scris articolul.

„Însă după ce [Rusia] a intrat în incapacitate de plată în 1999, tacticile prădătorilor şi ale agenţilor lor au devenit mult mai sofisticate. În prezent, de cele mai multe ori se întâmplă astfel: partea interesată dă ordin unei echipe specializate în vederea preluării companiei vizate. Agresorii încep de obicei prin a achiziţiona un pachet minoritar de acţiuni la firma-ţintă, pe care îl utilizează pentru a-i intenta acesteia procese mărunte. După aceea, încep un joc complex de-a arbitrajul pentru a compromite activităţile companiei şi a-i devaloriza acţiunile, ceea ce duce la un posibil faliment şi la preluarea aproape certă a acesteia."

Entitatea vizată în raidul împotriva lui Vrublevski a fost Fethard Finance, un sistem bazat pe monedă virtuală care nu mai există în prezent şi al cărui acţionar majoritar era Vrublevski. Prin intermediul unei entităţi juridice numite „Red & Partners", pe care o înfiinţase, Vrublevski a creat o reţea de siteuri de pornografie extremă. Crutop.nu, forumul on-line înfiinţat de Vrublevski („RedEye")*, era locul perfect pentru a face reclamă siteurilor Red & Partners către webmasterii ruşi de pornografie, care puteau primi comisioane din vânzarea de abonamente lunare la siteurile respective. (Amintiţi-vă că „Vergiliu" al nostru din lumea subterană a spammerilor – Vişnevski – a câştigat în tinereţe bani frumoşi din promovarea siteurilor afiliate Crutop.) Când webmasterii afiliaţi au fost plătiţi, plata nu s-a făcut în dolari sau ruble, ci în credite în moneda virtuală creată de Fethard, care a devenit rapid o formă acceptată de plată a bunurilor şi serviciilor în lumea subterană a criminalităţii informatice ruseşti.

Imperiul pornografic creat de Fethard şi Vrublevski a părut să funcţioneze perfect până în septembrie 2007, când Vrublevski – sau, mai exact, administratorul RedEye al lui Crutop – a anunţat peste opt mii de webmasteri ruşi care aveau bani

* De menţionat că Vrublevski neagă faptul că este RedEye, căruia îi spune întotdeauna „domnul RedEye", ceea ce este o glumă. Blogul lui Gusev despre Pavel se numeşte redeye-blog.com.

băgați în moneda virtuală că Fethard fusese ultima victimă a unui raid corporativ și nu mai rămăsese cu nimic.

Potrivit lui Gusev, eminența cenușie din spatele raidului a fost Mihail Jilenkov, soțul Mariei Okulova, nepoata celui dintâi președinte al Rusiei, Boris Elțin. Interesant este că tatăl Mariei, Valeri Okulov, a fost directorul general al Aeroflot – cea mai mare companie aeriană din Rusia, care avea să schimbe în curând și radical cursul existenței lui Vrublevski.

„În 2007, Fethard a avut doi acționari principali, pe Pavel și pe Jilenkov, un bine-cunoscut prădător cu relații în poliție și FSB", își amintea Gusev într-o convorbire telefonică. Aleksander Hinștein, jurnalist la revista rusească de informație *Moskovski komsomoleț*, a descris de altfel în amănunțime acțiunile întreprinse de RostInvest, o firmă de investiții a lui Jilenkov implicată în câteva scandaluri de preluare ostilă în a doua jumătate a deceniului trecut.



Gusev crede că setea de putere a lui Vrublevski și dorința sa de a se asocia cu oricine avea putere îl făcuseră pe fostul lui partener de afaceri să nu mai vadă ce anume îi aștepta. Jilenkov și-a folosit influența ca deținător a jumătate din companie pentru a prelua controlul asupra activităților cotidiene ale sistemului Fethard. În felul acesta, el a avut acces direct la toate conturile afiliate Fethard.

La 12 septembrie 2007, Vrublevski a fost atacat prin surprindere de două ori. Prima lovitură a primit-o când a aflat că practic toate conturile Fethard fuseseră golite, iar banii, transferați în conturi de la bănci offshore. A doua a primit-o când a descoperit că poliția rusă a început o anchetă penală împotriva lui și a lui Fethard, acuzându-i de activități bancare ilegale.

„Pavel fie nu și-a dat seama, fie nu și-a făcut griji în privința acelei laturi a personalității lui Jilenkov, pentru că se umfla în pene ca un curcan și se lăuda ce grangur era noul lui partener, ce relații și ce putere avea să-i aducă acesta", spunea Gusev într-o discuție cu autorul acestei cărți.

Raidul împotriva lui Fethard a fost un eveniment important fiindcă Vrublevski a ajuns să fie convins că a fost lucrat de Gusev. (Gusev neagă cu vehemenţă faptul că ar fi fost implicat, iar eu am ajuns să-l cred.) Hotărât să-i răspundă cu aceeaşi monedă celui pe care-l considera agresor, Vrublevski a început să se gândească împreună cu amintitul cofondator al Rx-Promotion, Iuri „Hellman" Kabaienkov, să pună autorităţile judiciare pe urmele lui Gusev.

„Jilenkov a fost cel care a stat la originea acestui dosar, a spus Gusev. A vrut să-l avertizeze pe Pavel să nu încerce să recupereze banii. Jilenkov a spus foarte clar că, dacă Pavel încerca să recupereze banii furaţi de la Fethard, va avea şi mai multe probleme, iar ancheta penală va continua. Pavel a bănuit însă mereu, în mod greşit, că eu am fost cumva implicat în treaba asta."

Motivul nu e greu de înţeles. Gusev şi Vrublevski sunt cum nu se poate mai diferiţi. Gusev este meditativ, erudit, prevăzător, autocritic şi zgârcit. În schimb, Vrublevski este vulgar, impulsiv, locvace, lăudăros şi risipitor. Gusev se descrie ca fiind un „bărbat de succes", care a crescut într-o familie bogată – bunicul lui a fost ministrul construcţiilor în fosta Uniune Sovietică – şi a primit o educaţie clasică la una dintre şcolile ruseşti de vârf.. Vrublevski, care pare cu cel puţin zece ani mai bătrân decât este în realitate – are în jur de 35 de ani – a fost mai puţin protejat în copilărie şi a fost exmatriculat din mai multe şcoli.

Gusev spunea că a început să lucreze în industria internetului în 1998, când un afacerist local i-a cerut să creeze un site pentru o afacere cu suveniruri sportive. Gusev a învăţat cât a putut despre programarea HTML şi web, câştigând 200 de dolari pentru ce a făcut. La scurt timp după aceea, şi-a zis că ar putea câştiga mai mult din pornografie, aşa că a angajat un programator care să-l ajute să creeze software capabil să alcătuiască liste cu siteurile pornografice utilizate în aşa-numitele operaţiuni „circle jerk".

„CJ, cum sunt numite acestea, sunt un fel de sistem în care diferitele siteuri care găzduiesc un număr mare de imagini pornografice îi redirecționează spre un site asemănător pe vizitatorii care dau clic pe o imagine, spunea Gusev. La baza sistemului stă ideea că ești redirecționat de atâtea ori, încât, până la urmă, obosești să mai cauți ce te interesează și dai clic pe unul dintre anunțurile plătite ca să cumperi un abonament. Este un sistem conceput să tocească răbdarea oamenilor, funcționând destul de bine, cel puțin o vreme. Îți pot spune însă că a fost un truc încercat pentru prima dată în SUA. N-a fost inventat în Rusia!"

Gusev și Vrublevski au făcut cunoștință datorită legăturilor comune cu pornografia extremă. În 1998, Gusev era administratorul unui forum on-line rusesc care se adresa webmasterilor ce comercializau filme și imagini care redau acte de bestialitate și acte sexuale cu animale domestice. Piața lui Vrublevski, pe care o servea prin intermediul holdingului său Red & Partners, o formau persoanele pasionate de pornografie violentă, cărora le place să vadă mai ales imagini și filme scurte în care sunt înfățișate violuri sau alte forme de sex forțat, incest și sodomie.*

Gusev a reușit să profite de afacere pentru că deținea o firmă de facturare a tranzacțiilor cu card de credit numită Digital Internet Billing, pe scurt „DiBill". Aceasta se baza pe o serie de relații cu sistemul bancar din Olanda, unde, potrivit lui Gusev, locuiau fericiți mulți dintre cei cărora li se adresa produsul companiei sale.

Într-o zi, Gusev a primit un mesaj de la Vrublevski, care-i cerea să se întâlnească și să discute despre combinarea

* Vrublevski neagă până și faptul că ar fi fost asociat cu compania-mamă care deține toate aceste siteuri, deși în actele de constituire apare aceeași adresă din Olanda care apare în actele de constituire a ChronoPay. Mai mult, siteul Red & Partners a fost găzduit multe luni la o adresă de internet atribuită companiei ChronoPay de către autoritățile europene de profil.

eforturilor lor și crearea unei societăți de procesare a plăților pentru industria pornografică aflată în plină expansiune, care înflorise practic peste noapte odată cu adoptarea pe scară largă a internetului comercial în Occident.

„Am discutat de câteva ori la Moscova. Părea foarte entuziasmat și motivat de această afacere nouă, ChronoPay. Mi-a spus că aș putea să fac echipă cu el, afirma Gusev. M-am gândit că putea fi un foarte mare pas înainte în cariera mea. Era bine să fi fost un pic mai deștept și să-i fi refuzat propunerea."

În 2003, cei doi au oficializat relația. Red & Partners s-a unit cu firma DPNet a lui Gusev, formând o nouă corporație în Olanda. Așa s-a născut ChronoPay. Printre investitori s-a numărat Vladimir Țasțin, directorul executiv al EstDomains, firma estoniană care rezervă nume de domenii pe internet. Țasțin și Vrublevski s-au împrietenit repede și, în următorii cinci ani, EstDomains avea să devină cel mai popular registru de domenii printre webmasterii ruși (în special cei care se ocupau de spam și malware).*




* Țasțin a respins ca „prostii" afirmațiile conform cărora EstDomains ar fi încercat să intre în grațiile spammerilor și furnizorilor de malware. Cu toate acestea, autoritățile de reglementare a activității pe internet aveau să-i retragă companiei capacitatea de a aloca noi nume de domenii după ce, într-un articol din *Washington Post*, s-a afirmat că Țasțin fusese condamnat în Estonia, printre altele, pentru tentativă de fraudă cu carduri de credit, spălare de bani și fals. EstDomains a încetat să mai existe după aceea, însă Țasțin și alți șase asociați se pare că și-au continuat activitățile ilegale. În 2011, acesta a fost arestat de autoritățile estoniene într-o operațiune internațională care viza dezmembrarea lui DNSChanger Trojan. Acest botnet uriaș infectase peste patru milioane de PC-uri din toată lumea cu malware care deturna rezultatele căutărilor și dezactiva softwareul de securitate. De pe urma lui, Țasțin și partenerii săi de afaceri câștigaseră peste 14 milioane de dolari. Aceștia au fost acuzați de fraudă și spălare de bani, dar, la sfârșitul anului 2013, au fost achitați de un tribunal estonian. În momentul scrierii acestor rânduri, ei așteaptă să fie extrădați din Estonia pentru a fi judecați în SUA, unde sunt acuzați

Pentru puțin timp, Gusev și Vrublevski au lucrat unul lângă altul în același birou, dar, după nici un an, se certau întruna cu privire la direcția pe care trebuia s-o urmeze firma. După un dezacord prelungit cu privire la cine avea să poată cumpăra acțiunile lui Gusev la ChronoPay, Gusev a vândut DPNet omului de afaceri rus Leonid Mihailovici Terehov și a început să se ocupe de GlavMed și SpamIt.

„Stăteam în același birou, față în față și cred că, din acest motiv, eram considerați prieteni sau parteneri de afaceri, a spus Gusev într-o discuție din 2011. Dar asta a ținut numai în primele cinci–șase luni. După aceea, am început să avem unele dificultăți de comunicare. Problema era că eu nu susțineam deciziile lui, iar el nu susținea deciziile mele."

Între timp, ceva ciudat se petrecea cu ChronoPay. Compania începuse să atragă afaceri legitime – nu doar siteuri pornografice, ci și companii de marcă din Rusia care doreau să-și ajute clienții să găsească posibilități alternative de a plăti pentru mărfurile cumpărate de la ele. Pe atunci, puțini ruși din clasa muncitoare utilizau sau măcar aveau card de credit și, cu toate că exista un interes tot mai mare pentru comerțul electronic, surprinzător de puține companii care făceau afaceri în Rusia erau dispuse și capabile să-i ajute pe consumatori să-și utilizeze conturile bancare pentru a plăti on-line.

Până în 2006, ChronoPay atrăsese în calitate de clienți mai multe firme importante din Rusia, inclusiv furnizorii de servicii de telefonie mobilă MTS și Skylink, și chiar organizații nonprofit cu orientare occidentală, ca World Wildlife Fund. Brusc, milioane de ruși au putut să plătească on-line facturile la încălzire sau telefon ori să cumpere bilete de concert și avion prin ChronoPay.

Gusev spunea că, prin atragerea acestor clienți mari, legali, Vrublevski voia să se asigure probabil că firmele din zona neagră și gri a economiei vor avea acces permanent la sistemele

de fraude informatice. [În 2016, Țastin a fost condamnat de un tribunal american la peste șapte ani de închisoare (n. red.).]

bancare dispuse să proceseze tranzacții mai riscante, precum achizițiile făcute de la farmaciile on-line și tranzacțiile cu carduri de credit legate de vânzările de software antivirus bazate pe șantaj.

„Principalul motiv pentru care ChronoPay a avut un asemenea succes atât de mult timp în toate aceste zone gri și negre ale economiei este că a avut un grup de clienți albi, ale căror afaceri reprezentau o acoperire pentru tranzacțiile gri și negre, spunea Gusev. Compania se folosea de asta pentru a obține tarife de procesare mai bune de la bănci, pentru că le spunea: «Vă vom aduce tranzacții de milioane de dolari de la unele dintre cele mai mari companii rusești, iar tot ce trebuie să faceți este să ne ajutați să le procesăm.»"

Stefan Savage, profesor la University of California din San Diego, care a făcut sute de cumpărături legale de medicamente de la farmacii administrate de GlavMed, Rx-Promotion și alte zeci de *partnerka*, a afirmat că, de fapt, ChronoPay nu procesa carduri de credit, ci mai degrabă promova și revindea servicii de plată (era un furnizor de servicii de plată, PSP – *payment service provider*).

„Nu avea relații bancare, dar colabora cu alte companii care aveau astfel de relații, spunea Savage. Avea multe înțelegeri cu persoane care o ajutau să facă rost de bani. ChronoPay reprezenta clienți falși, care vindeau medicamente prin intermediul unor bănci diferite, iar afacerile Rx-Promotion erau trecute pe rând prin companiile-paravan pe care le crease. Ulterior, după ce băncile își dădeau seama ce se întâmpla, ChronoPay nega faptul că știuse ce făceau companiile-paravan."

Cu alte cuvinte, ChronoPay și Vrublevski au jucat un rol esențial în crearea acoperirii organizatorice, legale și tehnice de care spammerii aveau nevoie ca să poată accepta carduri de credit pentru medicamentele pe care le promovau. ChronoPay și Vrublevski au folosit de asemenea aceleași tehnici pentru a ascunde rolul-cheie jucat în vehicularea a zeci de milioane de dolari prin intermediul plăților cu card de

credit de la americanii și europenii care au căzut victimă unor escrocherii de tip scareware. Așa cum vom vedea în capitolul 9, Vrublevski susține că, în ceea ce privește escrocheriile de tip scareware, el a fost doar un consilier care a ajutat afacerile implicate să creeze companiile-paravan și sistemele de plată necesare, astfel ca întreaga operațiune să pară legală companiilor de carduri de credit.

Potrivit afirmațiilor lui Savage, serviciul prestat de ChronoPay este cunoscut în domeniu sub denumirea de „factoring". Firma acceptă mai mulți clienți, asigură procesarea cardurilor de credit ale acestora și apoi le înregistrează tranzacțiile în conturi în numele companiilor fictive create de ea, pe care le prezentase băncilor ca fiind adevărații clienți. După aceea, Vrublevski și alți angajați ai ChronoPay implicați în afacere îi plăteau pur și simplu pe acești clienți din buzunarul lor.

Pe scurt, organizații suspecte apelau la ChronoPay mai ales când nu prea aveau alte variante.





„Au fost dispuși să preia și să se ocupe de toți acești clienți cu adevărat dubioși, care nu aveau să fie acceptați de nimeni altcineva, spunea Savage. Se făceau multe jocuri cu câțiva parteneri bancari, iar ChronoPay era foarte pricepută la acestea."

Parteneriatele respective – în special cu instituții financiare din fostele republici sovietice Azerbaidjan, Georgia și Letonia – au contribuit cel mai mult la dominația ChronoPay în domeniul procesării tranzacțiilor pentru farmaciile ilicite de pe internet și escrocheriile de tip scareware care aveau loc în spatele fațadei legale a companiei. Din fericire pentru Vrublevski și Gusev, această activitate a fost în general eclipsată o vreme de volumul mult mai mare al tranzacțiilor provenite de la companii rusești legale.

„ChronoPay este o companie unică dintr-un anumit punct de vedere, fiind renumită în Rusia pentru [asocierea cu] branduri rusești importante, a afirmat Gusev într-o convorbire din 2010. Toată lumea știe însă cine e proprietarul companiei, ce a făcut el înainte și ce face în acest moment."

La doi ani după ce Vrublevski și Gusev au apucat-o pe căi diferite în afaceri, Gusev a avut parte el însuși de succes. GlavMed și SpamIt încasau milioane de dolari pe lună și colaborau cu unii dintre cei mai iscusiți programatori din Moscova.

Ca să nu fie mai prejos ca rivalul lor, Vrublevski și Hellman aveau să lanseze, în 2007, Rx-Promotion, încercând să-i ademenească pe mulți dintre cei mai buni spammeri de la SpamIt. Deși intra într-un domeniu deja aglomerat, în care operau vreo 20 de alte *partnerka* farmaceutice ilicite, Rx-Promotion avea să beneficieze de la bun început de un avantaj față de concurenții săi, specializându-se în vânzarea de medicamente eliberate pe bază de rețetă, supuse unor restricții severe și care creează dependență – ca hidrocodonă și Valium. Medicamentele respective erau oferite tuturor clienților, indiferent dacă aveau sau nu aveau rețetă de la medic.

Gusev spunea că, inițial, GlavMed a oferit și medicamente controlate, dar a ajuns repede la concluzia că piața respectivă era prea volatilă și riscantă.

„Când GlavMed a început să funcționeze în 2006, existau unele substanțe controlate, dar, atunci, nu am înțeles în ce anume ne băgăm, spunea Gusev. După doi ani, am luat decizia strategică de a nu avea nicio legătură cu ele. La urma urmelor, dacă vinzi Viagra, nu afectezi grav sănătatea cuiva. Dar medicamentele controlate... dacă le vinzi pe internet, de cele mai multe ori le vinzi unor persoane dependente. Iar eu, sincer, nu vreau să fiu un fel de traficant de droguri."

Povestea lui Gusev nu se potrivește cu informațiile scurse de la SpamIt și GlavMed, care arată că cele două *partnerka* au continuat să vândă medicamente controlate, eliberate pe bază de rețetă cel puțin până la jumătatea anului 2009.

Toate indiciile arată că, în ciuda faptului că Vrublevski l-a avertizat din timp în privința mașinațiunilor politice și legale

pornite împotriva sa – Gusev a subestimat determinarea fostului său partener sau n-a putut găsi aliați care să aibă relațiile necesare în aparatul politic și juridic al Rusiei pentru a stopa ancheta penală îndreptată împotriva lui și a afacerilor sale. În primul rând, Gusev n-a început să-și ia măsuri de precauție pentru a dejuca manevrele lui Vrublevski decât la începutul lui 2010, când a acceptat în sfârșit că era anchetat de agenți ai FSB și că aceștia încercau să-l înfățișeze ca pe „spammerul nr. 1 al Rusiei".

Ancheta împotriva lui Gusev a coincis cu eforturile președintelui rus de atunci, Dmitri Medvedev, de a atrage investiții străine pentru „Skolkovo", un ambițios proiect de creare a unui parc tehnologic la marginea Moscovei, un fel de versiune rusă a Silicon Valley, cel mai mare incubator de inovații de înaltă tehnologie din SUA. Proiectul Skolkovo a căpătat amploare în martie 2010, după ce producătorul de hardware pentru internet Cisco Systems Inc. s-a angajat că va investi 1 miliard de dolari, iar compania de capital de risc Bessemer Venture Partners din Silicon Valley a promis investiții în valoare de 20 de milioane de dolari pe parcursul a doi ani.

Medvedev și alți lideri știau însă că, pentru a putea să atragă mai multe investiții din țările occidentale, trebuiau să spele imaginea Rusiei de țară tolerantă față de infractorii informatici de pe teritoriul său. În acest sens, Gusev era țapul ispășitor perfect. El avea să fie prima țintă importantă a Comitetului Național Anticorupție, un organism care avea scopul de a ajuta agențiile și ministerele să-i îndepărteze pe funcționarii corupți, care închideau frecvent ochii la infracțiuni în schimbul șpăgii sau al unor „donații".

Parcă pentru a valida alegerea Comitetului Național Anticorupție, prima reacție a lui Gusev, amenințat cu insistență că i se va face dosar penal, a fost să încerce să-i mituiască pe funcționarii publici pentru a întârzia acțiunea, a-i furniza amănunte despre mersul anchetei și a interveni în numele lui.

La 9 ianuarie 2010, Gusev l-a contactat pe Dmitri Stupin, coadministratorul lui GlavMed–SpamIt, prin intermediul chatului on-line, pentru a discuta despre posibilitățile de a evita sau de a amâna punerea lui sub acuzare. Gusev i-a spus că ar putea să cumpere protecție împotriva acuzațiilor vărsând diverse sume în conturile unor politicieni importanți care aveau influență asupra anchetatorilor.

Mai exact, Gusev a spus că ar putea deveni sponsor al Federației Ruse de Volei. Prețul cuprindea o taxă oficială de sponsorizare de 10 milioane de ruble (aproximativ 350 000 de dolari), plus 150 000 de dolari în bani gheață. Șeful federației, Nikolai Patrușev, este un om puternic în domeniul aplicării legii în Rusia: între 1999 și 2008, a fost director al FSB, organizația care a succedat KGB, iar apoi secretar al Consiliului de Securitate din Rusia.

Potrivit afirmațiilor lui Gusev, se obișnuiește ca federațiile sportive și organizațiile de binefacere rusești să fie folosite pentru dirijarea banilor spre buzunarele factorilor de decizie politică.

„În Rusia, sportul nu e tocmai o afacere, ci o modalitate de aranjare a afacerilor, spunea el într-o convorbire telefonică. Am un prieten care este un jucător de hochei destul de faimos. Odată mi-a spus că, în campionatul de hochei, există doar două echipe care ar putea câștiga ceva, pe când celelalte înregistrează doar pierderi. Sportul în Rusia este un fel de... dintr-un anumit punct de vedere, poți cunoaște oameni noi și poți începe o relație pentru viitor, iar dintr-un alt punct de vedere, poți obține un fel de protecție. Asta pentru că toate campionatele – de baschet, de fotbal, de hochei, de orice – sunt controlate cumva de persoane din guvern."

Există multe dovezi în sprijinul celor afirmate de Gusev. Un exemplu se găsește într-o carte scrisă de Lennart Dahlgren, fostul șef al diviziei ruse a producătorului suedez de mobilă IKEA. În *Despite Absurdity: How I Conquered Russia While It Conquered Me*, Dahlgren afirmă că a trebuit să dea șpagă

30 de milioane de ruble (1 milion de dolari) organizațiilor de binefacere ruseşti care au făcut ca banii să ajungă la funcționari publici şi înalți reprezentanți ai statului.

În mai 2011, Gusev mi-a spus, într-o discuție purtată la telefon, că a fost sponsor al campionatului rusesc de volei în speranța că va convinge pe cineva să oprească ancheta penală începută împotriva sa. Gusev era convins, iar documentele sustrase par să confirme acest lucru, că autoritățile au fost interesate de activitățile lui după ce au fost cumpărate de Pavel Vrublevski, fostul său partener de afaceri devenit concurent.

Într-adevăr, la sfârşitul anului 2010, Vrublevski a obținut pentru ChronoPay un contract de sponsorizare a Federației Ruse de Baschet. Federația de baschet este condusă de Serghei Ivanov, fost ofițer KGB, desemnat de preşedintele rus Vladimir Putin în calitate de viceprim-ministru al Rusiei. De fapt, compania ChronoPay a folosit legăturile cu Ivanov pentru a face publicitate succesului şi puterii dobândite de ea. Între fotografiile directorilor ChronoPay de pe blogul companiei există una cu Vrublevski şi Ivanov stând în picioare în primul rând la un meci de baschet, susținându-şi echipa, amândoi îmbrăcați în costum şi zâmbind cu toată gura.

Nu se ştie cât a trebuit Vrublevski să plătească pentru a obține acel contract de sponsorizare, dar există câteva indicii că suma a depăşit 1 milion de dolari. În martie 2011, într-un articol apărut în ediția tipărită a cotidianului rus *Kommersant,* se afirma că bugetul federației de baschet a crescut la aproximativ 6 milioane de dolari grație contribuției sponsorilor: ChronoPay, grupul de investiții rus VTB şi constructorul auto Sollers. În articolul respectiv, Ivanov era citat spunând că VTB a asigurat mai mult de jumătate din buget, iar cealaltă jumătate a fost asigurată de ChronoPay şi Sollers.

„Dacă doreşte să fiu numit spammerul numărul unu al lumii, Pavel plătește o grămadă de bani ca să mi se spună astfel, dar să ştii că n-am încercat niciodată să aflu cine a fost cu adevărat spammerul numărul unu", spunea Gusev. El se

referea la un studiu recent al cercetătorilor de la UCSD, care constatau că spammerii care lucrau pentru Rx-Promotion distribuiseră de două ori mai mult spam decât orice alt program, inclusiv SpamIt.

„Am crezut că trebuia să fie vorba despre proprietarii celor mai mari botneturi și m-am gândit că majoritatea lor colaborează cu SpamIt, spunea Gusev. Studiul arată însă că 25% din spam a fost pentru siteurile Rx-Promotion. Este foarte greu ca Pavel, cu toate informațiile, banii și influența pe care le posedă, să-i convingă pe oameni că problema principală n-o reprezintă chiar el."

Conversațiile de chat de la sfârșitul lunii ianuarie 2010 arată că Gusev și Stupin au făcut inițial federației de volei „donații" de 210 000 și 115 000 de dolari din partea companiei lor, Despmedia. O lună mai târziu, Gusev i-a spus lui Stupin că cheltuielile totale cu mita dată autorităților depășeau 400 000 de dolari.

Într-o conversație datată 19 februarie 2010, Gusev afirmă că tocmai a plătit 20 000 de dolari – 5 000 unui intermediar și 15 000 cuiva de la Procuratura Generală, organul care îl ancheta – pentru a primi informații și a „tărăgăna" ancheta. Gusev mai spune că a găsit pe cineva – un om foarte capabil, avocat și *reșalșik* (în stare să rezolve diverse probleme) – care putea oferi „servicii complete" pentru rezolvarea problemei „RedEye".

Persoana respectivă i-a promis că o donație adecvată ar asigura practic încarcerarea lui Vrublevski și distrugerea afacerilor lui dubioase. Prețul era însă destul de ridicat: 1,5 milioane de dolari.

Gusev spune că a cunoscut un *reșalșik* și îl întreabă pe Stupin ce să-i ofere pe lângă cele 1,5 milioane de dolari. Intermediarul vrea ca Gusev și Stupin să ajute o veche cunoștință comună să înceapă un program farmaceutic ilicit pe internet.

„Am găsit o persoană dispusă să mă ajute în această situație cu RedEye", scrie Gusev. „Tipul ăsta are un plan verificat, e un

avocat foarte tare. Unul care aranjează cu adevărat lucrurile. Pentru serviciile sale, în afară de o sumă foarte mare, cere ceva în schimb: să-l ajutăm pe amicul lui, un webmaster foarte cunoscut, care a avut o problemă similară celei pe care o avem noi și care a fost salvat de persoana respectivă. Acest «amic» nu face nimic în prezent. Avocatul ne cere să-l ajutăm să pună bazele unui program farmaceutic on-line. Pe mine nu mă încântă ideea de a crea mai multă concurență, dar, dintre toți cei cu care am vorbit, numai el a venit cu o soluție bine definită a problemei și ne-a dat o speranță."

Gusev vorbește apoi despre sponsorizarea federației de volei, adică despre cumpărarea agenților FSB corupți care trebuie să intervină în anchetă. „Oamenii de la asociația de volei ne pot proteja și vor face acest lucru folosindu-se de relațiile pe care le au în FSB, dar nu pot face mare lucru în cazul Procuraturii Generale. Nu vor putea decât să prelungească ancheta. De asemenea, nu-l vor putea acuza pe Red. Persoana pe care trebuie s-o ajutăm este vechea mea cunoștință, Pet, proprietarul lui [un termen colocvial pronunțat «lolnogo», care se referă la siteurile de pornografie infantilă] – care folosește facturarea cu ajutorul unor carduri speciale." Gusev se referă aproape sigur la Evgheni „Pet" Petrovski, proprietarul belarus al firmei de procesare a plăților Sunbill/BillCards, care a fost răpit de banda lui Loginov în capitolul 2.

După ce Gusev a spus că avocatul cere 1,5 milioane de dolari plus un serviciu personal, Stupin a exclamat: „Dumnezeule! Ce promite el pentru asta?"

„Promite că Red va rămâne în închisoare și nu-și va putea cumpăra eliberarea", a răspuns Gusev. „În plus, va pierde o mare parte din afacere și nu va mai avea bani ca să se mai războiască."

Într-o convorbire telefonică de la mijlocul anului 2011, Gusev explica astfel propriile acțiuni: „Nu am vrut decât să vorbesc cu cineva din FSB care se ocupa de cazul lui Pavel și

să-l conving să oprească tot acest conflict înainte de a fi prea târziu. Din păcate, asta nu m-a ajutat foarte mult."

În vara anului 2010, zeci de mii de e-mailuri și documente interne au fost sustrase de la ChronoPay de către persoane necunoscute din interior sau atacatori care au pătruns în mod neautorizat în rețeaua companiei – acestea conțineau nenumărate exemple de activități în care Vrublevski nu recunoscuse ani la rând că fusese implicat.

Când l-am întrebat dacă el a provocat acel incident, Gusev a negat, dar apoi a recunoscut că implicarea lui era o presupunere logică, având în vedere războiul de uzură care-l prinsese pe picior greșit.

„Pavel este cu un an înaintea mea fiindcă nu mă așteptam să facă publice toate aceste lucruri despre mine și despre afacerea noastră, a spus Gusev. Eu sunt un fel de infractor informatic și el este tot un fel de infractor informatic. Cel mai logic ar fi să rezolvăm discret această situație, dar el vrea atât de mult să-mi facă rău, încât ia decizii fără să le înțeleagă consecințele."

Convins că Gusev era cauza scurgerii în spațiul public a documentelor și e-mailurilor de la ChronoPay, Vrublevski a plătit un hacker local să spargă baza de date despre clienți a rețelelor SpamIt și GlavMed.

Următoarea conversație de chat este datată 28 august 2010, având loc la numai câteva zile după ce baza de date internă a SpamIt a ajuns în posesia autorităților din SUA. În această conversație, Stupin și Gusev discută despre închiderea rețelei SpamIt.

GUSEV: Se pare că am încurcat-o. Red a dat baza noastră de date americanilor.

STUPIN: Căror americani?

GUSEV: Nu știu exact, deocamdată. Probabil celor de la FBI sau Serviciului Secret. Ai citit pe blogul lui Krebs despre întâlnirea de la Casa Albă privind problema farmaciilor ilegale de pe internet?

STUPIN: Nu.

Gusev: krebsonsecurity.com/2010/08/white-house-calls-meeting-on-rogue-online-pharmacies.

STUPIN: Vrei să te întorci în Rusia?

GUSEV: Așa intenționez. Acum sunt realmente îngrijorat.

GUSEV: Crezi că „închiderea" va ajuta? Gândește-te numai: ei au TOATĂ baza noastră de date... Sunt 900 000 de înregistrări. Ce vom face cu ele? Ca să fim condamnați și să stăm cinci ani la închisoare, nu trebuie dovedită decât o singură tranzacție! Ce poate fi mai rău de-atât? La ei, condamnările se combină și e posibil să primim cinci condamnări la închisoare pe viață.

GUSEV: Și eu cred că trebuie să închidem afacerea, pentru că e un dezastru absolut!

GUSEV: În privința închiderii, cred că trebuie să închidem mai întâi SpamIt. Apoi, după o lună sau o jumătate de lună, GlavMed.





Gusev și Stupin aveau să închidă SpamIt.com la sfârșitul lunii septembrie a anului 2010, înlocuind pagina de pornire a Spamdot.biz cu următorul mesaj către afiliați:

> Din cauza numeroaselor evenimente nefericite care au avut loc anul trecut și a atenției tot mai mari acordate programului nostru de afiliere, am hotărât să oprim traficul începând cu 1.10.2010 [1 octombrie 2010]. Considerăm că este decizia cea mai potrivită în această situație. Evităm astfel încetarea bruscă a activității care ar duce la prăbușirea programului și la neplata profitului care vi se cuvine.
>
> În cazul nostru, întregul profit va fi plătit în mod normal. Sunt excluse orice posibile fraude. Vă rugăm să vă transferați traficul la alte programe de farmacii afiliate până la data de 1.10.2010.
>
> Vă mulțumim pentru cooperare! Apreciem foarte mult încrederea voastră!

Imediat după închiderea SpamIt, volumul de e-mailuri nesolicitate trimise la nivel mondial a scăzut considerabil – cu 20–40%, în funcție de estimări – deoarece spammerii care

colaborau cu rețeaua au încercat să-și mute traficul la alte parteneriate, care le puteau plăti serviciile. Experții care au urmărit cele mai importante botneturi de spam folosite pentru promovarea siteurilor farmaceutice „canadiene" din programul SpamIt au observat repede că majoritatea botneturilor importante – inclusiv Grum, Rustock și Cutwail – au fost trecute practic într-o stare neutră timp de câteva săptămâni, cât botmasterii au încercat să găsească modalități noi de a-și câștiga existența de pe urma mașinilor lor infracționale.

Datorită unui articol din *New York Times*, care, în conformitate cu e-mailurile sustrase de la ChronoPay, a fost scris pe baza unor informații furnizate de surse din departamentul de relații publice al Asociației Ruse a Comunicațiilor Electronice (ARCE), Gusev devenise cel mai mare spammer din lume, chiar dacă el susține că n-a fost niciodată un spammer în sensul propriu al cuvântului. În momentul în care poliția de la Moscova îi percheziționa apartamentul, Gusev fugise deja din Rusia cu soția și cu fiica lor, îndreptându-se, se pare, spre Spania.

Gusev nu avea însă de gând să cedeze fără luptă. În noiembrie, a lansat redeye-blog.com, un site pe care l-a utilizat pentru a prezenta publicului trecutul bogat în fapte al lui Vrublevski, angajând chiar un vorbitor nativ de limba engleză care să traducă blogul pentru cititorii din Occident. Nu a durat mult până când numeroșii inamici ai lui Vrublevski i-au urmat exemplul, etalând rufele murdare ale lui RedEye în comentariile postate pe blog. Sute de webmasteri de pornografie care aveau destule amintiri despre cele suferite din cauza lui Vrublevski au început să folosească blogul pentru a vorbi despre milioanele de dolari pe care acesta le datora încă după dezastrul Fethard.

„La Moscova este bine să locuiești când ai bani și prieteni buni, care te pot ajuta să-ți rezolvi problemele, spunea Gusev într-o discuție telefonică din noiembrie 2010. Eu încerc să distrug ChronoPay, care îi aparține, deoarece, dacă nu va avea bani, sper că va opri toate astea."

La scurt timp după acea discuție cu Gusev, Vrublevski a recunoscut în sfârșit că războiul farma, așa cum numeau mulți conflictul dintre ei, ajunsese într-un punct din care nu mai exista posibilitate de întoarcere. Mai exact, spunea Vrublevski cu ironie, niciuna dintre părți nu părea să fie descumpănită de „distrugerea reciprocă asigurată". Făcea referire la o doctrină a strategiei militare în care ambele părți angajate într-o cursă a înarmărilor nucleare sunt descurajate să lanseze un prim atac, din cauza certitudinii că o acțiune agresivă va declanșa un răspuns similar din partea celuilalt.

„Problema este că Gusev nu încearcă să mă lovească cu armele lui, ci încearcă să mă sperie, spunea Vrublevski într-una dintre numeroasele lui convorbiri telefonice cu autorul acestei cărți. Afirmația lui că s-a mutat în străinătate pentru totdeauna – astea-s prostii pentru webmasterii lui. Bineînțeles, totul pare a fi desprins dintr-un film cu James Bond, pentru că nimeni nu se ascunde așa. În realitate, Gusev așteaptă ca eu să-l sun și să-i spun: «Bine, omule, hai să încetăm războiul ăsta.» În *kompromatul* ăsta de la ChronoPay, nu există însă nimic care să mă poată determina să mă opresc sau care să-l poată salva. El crede că mă va putea șantaja astfel o dată la câteva luni, nimic altceva."

Între timp, consumatorii din întreaga lume se bucurau de scurta întrerupere a bombardamentului cu spam și malware, care amenința să le infecteze computerele și să le fure identitatea. Imperiul spamului ajunsese în pragul prăbușirii. Când l-am întrebat dacă nu-l îngrijora faptul că eforturile sale de a-l demasca și a-i crea neplăceri lui Vrublevski ar putea afecta și mai mult o industrie la construirea căreia contribuise el însuși și care-l făcuse foarte bogat, Gusev mi-a spus că acesta era un risc pe care trebuia să și-l asume.

„Cel puțin, amândoi vom pierde mult timp, multă putere și mulți bani și nu va exista un câștigător, mi-a spus el la telefon, dintr-un loc nedezvăluit din străinătate. Fac încă unele

afirmații pentru a continua acest conflict dintr-un singur motiv. Dacă mă opresc acum, peste un an sau doi, Pavel va găsi prilej să mă lovească din nou, din altă direcție, și nu vreau să-i permit asta."

L-am crezut pe Gusev când mi-a povestit despre viața lui, despre afacerea lui și despre conflictul lui cu Pavel. Poate că nu mi-a spus întotdeauna întregul adevăr, dar am avut puține motive să mă îndoiesc de versiunea lui cu privire la cele întâmplate. Pe de altă parte, în discuțiile noastre, Vrublevski m-a mințit adeseori sau a împins adevărul mult dincolo de limita credibilității. Chiar și așa, mi-a promis că va fi mai deschis dacă aveam să mă întâlnesc pe terenul lui și eram nerăbdător să aud povestea spusă de el. Era timpul să-mi reînnoiesc pașaportul.

# Capitolul 9

# ÎNTÂLNIRE LA MOSCOVA

Gheaţa de pe râul Moscova trosnea şi gemea, răscolită dedesubtul celor două motoare care propulsau cu viteză constantă spărgătorul nostru de gheaţă, un vas elegant şi modern de croazieră. Pe îndepărtatul ţărm, formidabilul edificiu al Kremlinului se înălţa deasupra apei negre, îngheţate. Cineva a deschis o uşă înapoia mea şi aerul înviorător al nopţii s-a umplut de sunetul discordant al dinamicei muzici uşoare ruseşti, al clinchetului paharelor şi al zăngănitului tacâmurilor pe farfurii.

Februarie nu este nicidecum luna cea mai potrivită pentru o călătorie în Rusia, dar o invitaţie primită în 2011 de la firma rusă de securitate informatică Kaspersky Lab s-a dovedit a fi prea tentantă ca s-o refuz. Voiam să-l surprind pe Vrublevski – şi nu eram sigur că avea să mai fie multă vreme un om liber – aşa că am dat curs invitaţiei.

Studiam limba şi cultura rusă – ca şi dedesubturile ei sordide de criminalitate informatică – de peste cinci ani şi visam de mult să vizitez această ţară. Am anunţat însă puţine persoane că voi pleca în Rusia şi n-am spus nimănui adevăratul motiv al călătoriei mele: să mă întâlnesc cu Pavel Vrublevski la Moscova şi, eventual, cu Igor Gusev într-un ocol prin Europa (pe care nu l-am mai făcut niciodată). Pe atunci, mă gândeam că disputa dintre ei putea fi subiectul unui articol interesant şi abia aşteptam să mă întâlnesc cu fiecare faţă în faţă.

Dorisem să-i cunosc pe infamii escroci informatici deoarece credeam că aceasta putea fi singura mea şansă de a vorbi cu ei personal, fără a ne afla în prezenţa unor gardieni. Mă pregăteam să postez o serie de articole în care prezentam dovezi ale războiului farma dintre Gusev şi Vrublevski, cei doi fiind responsabili probabil de circa 75% din spamul de pe planetă. Eram convins că niciunul nu va mai dori să discute cu mine după ce începeam postările.

„Brian! Vino, începe spectacolul", a strigat Eugene Kaspersky, afişând un zâmbet larg şi fluturând din mână. Abia reuşeam să-l aud din cauza zgomotului turbinelor şi a trosnetului gheţii de pe râu. Intrând după el pe uşa care ducea de la pupa în sala principală, aproape că m-am lovit de un grup de tineri în salopete bleu, care făceau roata şi executau un dans rusesc tradiţional în ringul dintre bar şi mese.

Croaziera cu Kaspersky a avut loc cu o zi înainte de plecarea mea de la Moscova. După ce ne-a fost servită cina, eu şi Kaspersky ne-am delectat cu câteva păhărele de votcă rusească rece ca gheaţa, iar el mi-a povestit despre munca desfăşurată în domeniul criptografiei în anii 1980, când a lucrat la un institut finanţat de Ministerul Apărării şi KGB.

Am descoperit că amândoi am devenit interesaţi de securitatea computerelor după ce am căzut victimă unor atacuri informatice. Eugene a devenit obsedat de viruşi când a descoperit malware în computerul său în 1991. Eu am început să învăţ tot ce se putea despre computere şi securitatea pe internet un deceniu mai târziu, când reţeaua de acasă a fost atacată de „viermele li0n", creat de un hacker chinez devenit faimos, care mi-a blocat accesul la PC şi a distrus câteva servere.

În timp ce-i priveam pe dansatorii care se agitau dintr-o parte în alta a sălii, m-am întors cu gândul la ziua sosirii mele la Moscova, când am încercat să stabilesc o întâlnire cu Vrublevski. După întrevederea mea cu faimosul personaj din lumea criminalităţii informatice, nu mai putusem să închid

un ochi și continuam să rememorez evenimentele petrecute în cursul zilei.

În drumul meu spre Moscova, am trecut prin Aeroportul Internațional „John F. Kennedy" din New York, unde m-am întâlnit cu jurnalistul și analistul Paul Roberts, care începuse de curând să lucreze pentru Kaspersky. Roberts mergea și el la Moscova.

Nu fusesem niciodată în Rusia, dar când ne-am apropiat de Aeroportul Internațional Șeremetievo, mi-am dat seama că Moscova era deocamdată așa cum mi-o imaginasem: posomorâtă, rece, acoperită de zăpadă și bătută de vânt.

Așteptând ca avionul să aterizeze, mi-am dat seama brusc cât de puțin mă pregătisem de fapt pentru această călătorie și, pentru prima dată, m-am speriat puțin. Înainte de plecare, un membru al familiei, care lucrase în diplomație, mi-a dat, fără să-i cer, câteva sfaturi legate de siguranță. O bună parte dintre poveștele lui erau realiste: „stabilește-ți toate întâlnirile în spații publice", „nu te duce nicăieri singur", „evită să intri într-o mașină cu necunoscuți". Am fost uimit să constat însă cât de repede aveam să fiu obligat să ignor toate aceste sfaturi după sosirea la Moscova.

Eu și Roberts ar fi trebuit să fim așteptați la aeroport de o mașină care să ne ducă la hotel, dar plecarea de la New York a fost întârziată de vântul puternic, iar când am ajuns în Rusia, nu ne mai aștepta nimeni.

După ce am ieșit din terminalul principal și am pășit pe trotuarul cu zăpadă pe jumătate topită, am fost imediat identificați ca americani și am fost acostați de șase–șapte bărbați, care s-au oferit să ne ducă „ieftin" cu taxiul de la aeroport. Din păcate, hotelul nostru era la 30 km de aeroport, iar cursa n-avea să fie deloc ieftină.

După foarte puțin timp de la ieșirea din terminal, am simțit că mi se face greață în asemenea măsură încât m-am gândit că voi vărsa micul dejun peste taximetriștii care îmi ațineau

calea și nu acceptau să-i refuz. M-am așezat pe o bancă de metal acoperită cu zăpadă pentru a mă liniști și a-mi reveni. Se pare că taximetriștii au simțit că ar putea să le pară rău dacă se vor apropia prea mult și m-au lăsat în pace vreo două minute. Roberts a venit agale la mine, după ce s-a uitat cu atenție într-o parte și-n alta, sperând să zărească mașina care fusese trimisă să ne ia.

„Nici pe mine nu mă încântă ideea, dar se pare că va trebui să apelăm la unul dintre tipii ăștia", a spus el, mijind ochii din cauza ninsorii puternice.

Cinci minute mai târziu, stăteam înghesuiți pe bancheta din spate a unui automobil rusesc, negru și mic, care a pornit în viteză pe străzile acoperite de zăpadă fleșcăită, ocolind mașinile care mergeau mai încet pe aglomerata Leningradskoie Șosse, principala arteră care duce de la aeroport în centrul Moscovei. Am profitat de ocazie pentru a testa serviciul preplătit de date mobile. Fiindcă folosesc rareori rețele publice wi-fi nesecurizate și eram și mai puțin interesat să fac asta la Moscova, am vrut să nu fiu la mila serviciilor wireless din cafenele sau de la hotel cât timp eram în oraș. De aceea, am achiziționat dinainte acces la internet de la o companie denumită XCom Global. Aceasta mi-a dat un adaptor USB de rețea chiar înainte de plecare, care ar fi trebuit, teoretic, să-mi asigure accesul la internet 3G aproape în orice loc din oraș.

Când am conectat însă adaptorul la Macbook pe bancheta din spate a taxiului, am constatat stupefiat că semnalul se tot întrerupea după câteva secunde. M-am gândit că asta se întâmpla probabil fiindcă goneam pe șosea cu 120 km/h, dar, ulterior, aveam să descopăr că serviciul era la fel de instabil și când stăteam într-o cafenea de lângă hotelul nostru, chiar în centrul Moscovei. Puținele planuri pe care mi le făcusem înainte de călătorie se năruiau cu repezîciune.

După 45 de minute și achitarea echivalentului a 170 de dolari, eu și Roberts am coborât din taxi și ne-am cazat la Hotelul „Marriott Grand" de pe strada Tverskaia, un bulevard larg

care începe din Piața Roșie și trece prin centrul Moscovei. La recepție, o tânără drăguță mi-a cerut pașaportul. După ce i l-am arătat, mi l-a luat, mi-a spus scurt că-l puteam ridica mai târziu în cursul zilei și apoi a dispărut într-un birou din spate.

Nu m-a încântat prea mult ideea de a renunța la pașaport, dar nici nu aveam alternativă. Neliniștea mea s-a transformat curând în groază. Sosisem doar de cinci ore, când am primit o alertă de la Google, pe care o creasem pentru a urmări postările de pe internet în care apărea numele meu. Alerta se referea la un mesaj scurt, postat pe serviciul de blogging LiveJournal din Rusia, care preciza unde anume mă aflam. Postarea suna astfel: „Brian Krebs, blogger american în domeniul securității informatice, se află acum în Rusia, la Marriott Grand din Moscova."

Am fugit în camera mea spațioasă de la hotel, am încuiat ușa și am început să mă întreb dacă nu făcusem o greșeală uriașă venind în Rusia. În cele din urmă, m-am convins că nu, amintindu-mi că interviul acesta era esențial pentru a încheia cercetarea întreprinsă cu scopul de a-i expune pe acești spammeri. După câteva ore, mi-am făcut destul curaj ca să-l sun pe Vrublevski. Mi-a răspuns la al treilea număr de telefon mobil pe care-l aveam de la el.

– Neniiiică! a strigat el în aparat. E șapte dimineața la tine acolo. Cine a murit?

L-am informat că mă aflam de fapt în fusul lui orar și că trebuia să ne întâlnim cât mai curând posibil. După alt „neniiiică" prelung, m-a anunțat că va trimite o mașină după mine și mi-a cerut să aștept în holul de la recepție. Mi-a spus că o va trimite împreună cu șoferul pe secretara lui, Vera. A descris-o apoi pe Vera ca fiind o doamnă mai în vârstă, neatrăgătoare și obeză, dar care vorbea englezește și știa cum să se poarte cu occidentalii.

Peste 15 minute, m-am așezat în hol și am așteptat-o agitat pe Vera, urmărindu-i pe oamenii care veneau, tropăiau pentru

a se scutura de zăpadă și intrau în hotel pe ușa turnantă. Stând acolo și sorbind dintr-o ceașcă ceai fierbinte, mi-a fost greu să nu trag cu ochiul la o brunetă superbă și zveltă, care stătea lângă ușă, cu un aer agitat, îmbrăcată în blugi mulați și o haină albă, pufoasă. După ce am încercat fără succes să nu mă uit spre ea, n-am putut să ignor faptul că și ea încerca să nu se uite fix la mine.

După vreo cinci minute de privit pe furiș, tânăra s-a apropiat de mine și m-a întrebat dacă mă cheamă Brian. Pe moment m-am alarmat (nu cunoșteam aproape pe nimeni în Moscova), până când ea mi-a spus că o cheamă Vera și mi-am amintit brusc, zâmbind în barbă, de ce nu puteam avea încredere în mai nimic din ceea ce spunea Vrublevski.

Gluma a continuat când, după ce ne-am târât 20 de minute prin Moscova la o oră de vârf, am ajuns la sediul ChronoPay și am dat nas în nas cu aceeași fată, îmbrăcată în alte haine. Se vede treaba că Vera avea o soră geamănă care lucra tot acolo.



În acea seară, Vrublevski era năucit de-a dreptul, iar vizita-surpriză pe care i-o făceam îl surescitase în mod evident. Fidel obiceiului său, s-a lansat într-o poveste alambicată aproape imediat ce am sosit. Se pare că cineva aranjase ca poliția să descindă la Rx-Promotion Gold Party, o petrecere organizată cu patru seri în urmă la Golden Palace din Moscova. Evenimentul, la care se consumă de obicei multă băutură și pornografie, este organizat pentru toți afiliații lui Rx-Promotion: cele câteva sute de persoane care promovează siteurile farmaceutice Rx-Promotion. Afiliatul cu cele mai bune rezultate era răsplătit cu un lingou de aur de un kilogram, iar ceilalți clasați pe locuri fruntașe primeau iPad-uri și iPhone-uri.

Din nefericire pentru afiliații Rx-Promotion, petrecerea s-a spart când bărbați cu cagule și pistoale automate au coborât din câteva autobuze, au pătruns în forță în sală și au început să-i interogheze pe participanți. Vrublevski susține că au fost

trimişi de autorităţile din domeniul combaterii traficului de droguri, însă, potrivit unor martori care au postat pe diverse forumuri imagini de la eveniment, poliţia pare să fi folosit descinderea ca pretext pentru a asocia identităţile on-line ale afiliaţilor Rx-Promotion cu chipuri şi nume reale. Îmi spun că versiunea lui Vrublevski este improbabilă, dar nu vreau să-l întrerup ca să nu se considere jignit şi să vrea să mă dea afară... sau mai rău.

Vrublevski n-a participat deloc la petrecere. El spune că, cu o zi înainte, soţia îl rugase în mod inexplicabil să plece numaidecât într-o vacanţă în Maldive. Mai mult, cineva avusese prezenţa de spirit să înlăture toate logourile Rx-Promotion din spaţiul închiriat pentru petrecere cu câteva ore înainte de sosirea poliţiei.

– Tot internetul rus ştia că la Moscova va fi o petrecere a reţelei Rx-Promotion şi, evident, toată lumea s-ar fi aşteptat să vadă logouri Rx-Promotion, îmi spune Vrublevski, fumând întruna Marlboro în sala mică destinată şedinţelor conducerii, în care se află un uriaş planiglob vechi, flancat de săbii şi un drapel roşu imens din epoca sovietică. Şi, desigur – a continuat el, vorbind despre sine la persoana a treia – toată lumea se aştepta să-şi facă apariţia domnul Vrublevski. Bineînţeles că domnul Vrublevski n-ar fi fost în stare să-i împiedice pe toţi nenorociţii care se învârteau pe acolo şi fotografiau cu telefoanele. De aceea, domnul Vrublevski a decis să nu participe. În acelaşi timp, altcineva a hotărât să elimine toate logourile Rx-Promotion. Domnul Vrublevski se duce cu avionul în Maldive pentru o vacanţă de o săptămână. Apoi primeşte un telefon şi i se spune că, la petrecere, vor sosi cinci autobuze cu forţe speciale ale serviciului antidrog, care vor închide Golden Palace şi două cafenele din apropiere pentru simplul motiv că sunt prea multe forţe speciale, câini şi aparate de fotografiat. Intră şi dau peste un mare rahat: nu este nici domnul Vrublevski, nu sunt nici logouri, nu este absolut nimic care să merite să fie filmat.

Povestea despre descinderea poliției la petrecerea organizată pentru Rx-Promotion cu scopul împroșcării cu noroi a fondatorilor și afiliaților rețelei a fost cu siguranță amuzantă, dar se pare că a fost pur și simplu una dintre cele nouă asemenea descinderi făcute la cazinouri și cele aproape o sută de descinderi la „sălile de jocuri de noroc" ordonate în 2011 de Anatoli Andreev, noul șef al brigăzii antipariuri din poliția Moscovei.

După ce îmi povestește acest episod aparent întâmplător, Vrublevski o roagă pe Vera să ne aducă niște cafea și începem să vorbim despre traficul din Moscova și despre bărbatul care tropăia deasupra noastră, aruncând cu lopata mormanul de zăpadă de pe acoperișul clădirii. Îl întreb pe Vrublevski câte ceva despre familia lui și îmi răspunde zâmbind cu subînțeles și râzând batjocoritor că tatăl lui a lucrat mulți ani la Nycomed, o mare companie farmaceutică europeană.

Îl întreb apoi despre originea sabiei de lângă drapelul sovietic aflat în spatele scaunului meu. Vrublevski îmi spune o poveste lungă despre cum i-a fost oferită de primarul capitalei Daghestanului, pe care îl consideră un prieten apropiat. Nu îmi spune numele lui, ci doar că a fost – cel puțin la un moment dat – primarul orașului Mahacikala. Potrivit celor de la *Moscow Times*, este vorba probabil despre Said Amirov, primar în patru rânduri, despre care se spune că a supraviețuit unui număr de peste 15 atentate și este paralizat de la brâu în jos. De asemenea, potrivit unui articol publicat în *Moscow Times* în februarie 2014, Amirov este în prezent [2014] judecat după ce a fost acuzat în 2013 de trafic ilegal de arme, prin urmare este destul de amuzant faptul că i-a dăruit lui Vrublevski o sabie.

– Se pare că unchiul tipului cu care am fost acolo era primarul orașului Mahacikala [capitala Daghestanului], și-a amintit Vrublevski. Primarul ăsta era omul cel mai atacat din lume. Fusese aruncat în aer de vreo 13 ori. N-a murit, dar este într-un scaun cu rotile. Odată, grupările teroriste locale

au aruncat în aer un cartier întreg, încercând să-l omoare. Nu doar o clădire, ci tot cartierul.

Vrublevski evită întrebările directe despre motivul pentru care s-a dus în acea republică muntoasă turbulentă, cu populație majoritar musulmană, care se învecinează cu Georgia și cu Cecenia separatistă. Este însă posibil ca el să fi trecut prin regiune venind de la Baku, din Azerbaidjan. E-mailurile din arhiva ChronoPay arată că directorii companiei au vizitat Baku în mai multe rânduri pentru a cultiva relația cu Bank Standard, o instituție financiară azeră care procesa un volum uriaș de plăți pentru programele antivirus dubioase ale ChronoPay și pentru siteurile farmaceutice ale Rx-Promotion.

Schimb subiectul și îl întreb pe Vrublevski dacă a aflat cine a fost responsabil de scurgerea pe e-mail a documentelor interne ale companiei ChronoPay.

– Scurgerea a venit din interiorul companiei, din departamentul IT, zice el. Și-au dat seama că vor fi prinși că fură bani. De aceea, mai întâi, au făcut praf sistemul de contabilitate internă, astfel încât acest *kompromat* a devenit inutil pentru autorități, deoarece pur și simplu nu mai avem o bază de date contabile. A fost distrusă înainte de scurgerea pe internet a *kompromat*-ului.

Am împins pe masă spre Vrubleski un dosar plin cu e-mailuri printate.

– Ei bine, cel care a făcut asta mi-a trimis aproximativ 30 000 de e-mailuri din arhiva internă a ChronoPay. Acestea au făcut parte din primul pachet de e-mailuri pe care l-am primit de la începutul lui 2009 până la jumătatea lui 2010.

Vrublevski frunzărește fără chef câteva pagini, ridică din umeri, apoi împinge dosarul înapoi pe masă.

– Nu mă surprinde deloc.

Răspunsul lui vag nu mă descurajează.

– Este o colecție destul de bogată de documente. S-ar putea să ți se pară interesante. Sunt multe lucruri acuzatoare și

niciunul nu e prea măgulitor pentru tine sau ChronoPay. Cred însă că ai văzut deja majoritatea acestor e-mailuri.

– Se poate. Sunt multe lucruri interpretabile acolo.

– Oricum ar fi, insist eu, documentele îmi arată că n-ai fost deloc cinstit cu mine, Pavel.

– Serios? În ce privințe? întreabă el într-o doară.

– În multe privințe. Pentru început, mai ții minte primul articol pe care l-am scris despre ChronoPay? Despre antivirusul din 2009? Ai spus că n-ai avut nimic de-a face cu acel domeniu.

– Da, și care-i treaba?

– Păi, tu să-mi spui! Din câte îmi dau seama, treaba este că voi ați pus pe picioare o întreagă industrie a criminalității informatice, ați cumpărat domenii și ați lucrat pentru ea.

– Așa, și? Ți-am spus despre asta și înainte: asta fac toți procesatorii și nimeni nu îți poate spune acest lucru dintr-un motiv foarte simplu – încalcă regulile Visa și MasterCard. Visa și MasterCard știu că toți procedează așa, dar, potrivit regulilor, este ilegal. Înregistrarea ID-urilor comercianților face parte din serviciul pe care îl furnizezi. În plus, asiguri asistență pentru clienți, care este legată de serviciu.

Terminându-și cafeaua și aprinzându-și altă țigară, Vrublevski se referă la articolul publicat de mine în 2009 în *Washington Post*, în care stabileam multe legături între el, ChronoPay și industria antivirușilor dubioși.

Nu-mi puteam crede urechilor; Vrublevski recunoscuse că multe dintre companiile pe care ChronoPay susținea că le reprezintă ca fiindu-i clienți fuseseră de fapt constituite și conduse de angajați ai ChronoPay.

– Aici greșești tu. În perioada care are legătură cu articolul tău, noi nu știam prea multe despre spyware. Dar compania pe care o urmăreai tu nu era utilizată doar pentru spyware. Era utilizată pentru o grămadă de prostii. Poți să te duci și să cercetezi la Wirecard și Visa Islanda și-o să găsești aceleași prostii. Motivul este acela că, atunci când deschizi un ID de comerciant, trebuie să-l înregistrezi la o companie, care trebuie

să pară extrem de solidă pentru cei din exterior, asemenea unui site legal și așa mai departe. Așa că, în cazul majorității furnizorilor de servicii de plată, în principiu îți înregistrezi tu însuți companiile și le urmărești din interior.

– De asemenea, nu mi-ai spus niciodată că ChronoPay a prelucrat plățile pentru Rx-Promotion... am replicat eu.

– Așa-i, ai dreptate. Nu ți-am spus.

– Dar este adevărat, nu-i așa?

– Da. Mă rog, mai precis a fost adevărat.*

Răspunsul lui m-a surprins.

– Ce vrei să spui? Nu mai este? De când?

– Prietene, dacă ți-aș fi putut spune asta, aș fi fost foarte fericit.

– Asta-i tot? Care-i treaba, Pavel? Știi bine că am făcut cale lungă, cu mari riscuri, ca să te intervievez aici personal. Nu-i deloc frumos din partea ta să te porți așa.

Știam că risc să-l întărât, dar aveam nevoie de răspunsuri.

Râzând din nou, mi-a zis:

– Am renunțat la ei, nu mai sunt clienții noștri. Foarte simplu.

– La Rx-Promotion? Când?

– În septembrie 2010. Am avut așadar... o jumătate de an la dispoziție ca să iau decizii de afaceri legale.

Vrublevski dă un telefon și, vorbind în rusă, îi cere Verei să ne mai aducă niște cafea.

– Persoanele care au trimis documentele despre compania ta, insist eu, au multe informații despre afacerile tale.

– Furau bani de aici, bineînțeles că au informații. Dar nu vor ajunge nicăieri cu asta.

* În sfârșit, ajungeam undeva. Faptul că Vrublevski recunoștea că firma lui fusese de fapt puternic implicată în colaborarea cu Rx-Promotion confirma ceea ce reieșea în mod evident din examinarea e-mailurilor și documentelor sustrase de la ChronoPay. În una dintre lungile noastre convorbiri telefonice avute înainte de a-l vizita la Moscova, Vrublevski a recunoscut efectiv că acele documente și e-mailuri erau valide, declarându-mi fără chef că le-ar fi fost greu până și celor din FSB să falsifice atâtea documente câte se scurseseră din arhiva ChronoPay.

– De ce?

– Vezi tu, *kompromat*-ul nu e suficient ca să nenorocești pe cineva. Trebuie să și poți dovedi ceva, iar pentru asta trebuie să știi cum merge treaba. Cei care au făcut publice informațiile astea au comis o mulțime de greșeli. Eu răspândesc informații cu mare atenție. În principiu, poți să-ți dai seama cine răspândește informațiile nu din informațiile respective, ci din informațiile din jurul lor. Tu știi ceea ce ei nu știu. Îți poți da seama foarte simplu cine a făcut-o, pe baza a ceea ce știe și a ceea ce nu știe el.

Zâmbindu-ne neliniștită amândurora și simțind că discuția a devenit cumva mai încordată, frumoasa Vera intră cu băgare de seamă în sala de ședințe, ne pune înainte ceștile de cafea și iese repede. Răspunsul lui Vrublevski m-a pus în încurcătură, dar nu vreau să-l întrerup.

– Bine, am spus. Continuă.

– Brian, există ceva care n-are legătură cu subiectul ăsta... ceva care mă surprinde.

– Ce anume?

– Când vine vorba despre mine... de ce te aștepți ca eu să fiu sincer? Te rog să-mi amintești.

M-a surprins puțin modul inteligent în care a făcut ca discuția să se concentreze asupra mea.

– Poți spune că sunt de modă veche. Cred că, atunci când pun o întrebare directă, aștept un răspuns cinstit.

– Ha, ha, ha. Mulți așteaptă asta. Revenind la subiect, nu mi se pare că Rx-Promotion sau multe alte prostii din *kompromat* ar fi cine știe ce problemă. Și-ți spun de ce: de fapt, eu nu încalc prea multe legi.

Auzind asta, izbucnesc fără să vreau în râs atât de tare, încât cafeaua pe care tocmai o sorbisem aproape că îmi țâșnește pe nas. Abia reușesc să n-o împrăștii pe costumul meu și pe masa din sala de ședințe. Amândoi râdem din toată inima, ceea ce contribuie la destinderea atmosferei.

Îmi dădeam totuși seama că această manieră de abordare nu va fi fructuoasă. Am încercat să o schimb și am scos din servietă alte e-mailuri printate de la ChronoPay.

– Vreau să-ți văd reacția la acest e-mail expediat la 16 martie 2010 de Vladimir Stepkov, șeful securității de la ChronoPay, având ca subiect „câștiguri totale Rx-promotion2". Se pare că se referă la faptul că ești proprietar la Rx-Promotion împreună cu Iuri „Hellman" Kabaienkov. Spune așa: „Oameni buni, iubitul nostru Kisilev a anunțat datele cu privire la costul asistenței tehnice. Pavel și Hellman împart totul în jumătate și..."

Vizibil deranjat, Vrublevski mă întrerupe și nu mai zâmbește.

– Oho, Brian, oho, stai! Habar n-am ce se-ntâmplă aici! Nu pot intra prea mult în detalii referitoare la discuțiile dintre alții și mine. Așa că, dacă vrei să renunți la întrebările astea sperietoare, ar fi mai bine, poate, să trecem la discuții normale.

Tac câteva minute. Vrublevski zâmbește din nou afectat și își aprinde altă țigară înainte s-o fi terminat pe cea pe care o fuma. Îmi spun că o tăcere apăsătoare l-ar putea determina să divulge mai multe lucruri. Nici gând însă.

– N-o să intru prea mult în prostia ăsta cu Rx-Promotion, iar tu n-o să reușești să afli prea multe singur. Același lucru este valabil pentru spyware. Fac însă o treabă mai bună în privința lui Gusev. Așa cum spun sticleții, cel mai bun mod de a afla ceva este când omul spune acel lucru cu gura lui. Nu vreau să vorbesc despre asta. Ți-am făgăduit însă că-ți voi răspunde sincer la unele întrebări. Bineînțeles, nu la toate, doar la unele dintre ele.

– Am înțeles. Perfect, vrei atunci să-mi faci un serviciu, te rog? Anunță-mă când vrei să începi să faci asta.

Am discutat mai bine de trei ore, iar întrebările mele directe au primit răspunsuri la fel de evazive și lipsite de sens din partea lui Vrublevski. Epuizat, mi-am strâns în cele din urmă lucrurile și i-am mulțumit pentru timpul acordat. La plecare, Vrublevski m-a plimbat prin clădirea în care se aflau

birourile ChronoPay şi care, potrivit spuselor lui, era un edificiu cu valoare istorică.

Când am coborât scările spre parcarea de la subsol, mi-a arătat o uşă aflată exact cu un etaj mai jos de intrarea în biroul ChronoPay. Pe plăcuţa de pe uşă scria: „Asociaţia Rusă a Comunicaţiilor Electronice". ARCE este o firmă de lobby, al cărei principal organizator, potrivit documentelor scurse din arhiva ChronoPay, primea un salariu lunar de la ChronoPay. Era aceeaşi ARCE care preluase iniţiativa în campania desfăşurată de mass-media occidentală împotriva lui Gusev, considerat de aceasta „spammerul nr. 1 din Rusia".

Am părăsit Rusia două zile mai târziu, după ce am refuzat alte două invitaţii din partea lui Vrublevski de a ne vedea. Întâlnirea noastră mă iritase şi mă descurajase. În ultimele opt luni, îl ascultasem spunându-mi la telefon tot felul de minciuni, dar văzându-l acum făcând acest lucru într-un mod atât de flagrant şi deschis, fără să se ferească, m-am simţit extrem de stânjenit în prezenţa lui.



Nu mă aşteptasem la multe de la el, aşa că n-am fost foarte surprins când a evitat să dea răspunsuri directe la interviu. A confirmat totuşi câteva informaţii importante. ChronoPay era nu doar profund implicată în procesarea plăţilor pentru companiile de antiviruşi falşi şi pentru parteneriatul Rx-Promotion, ci şi responsabilă în primul rând de crearea şi dezvoltarea acestor afaceri.

Siguranţa exagerată cu care Vrublevski a spus că nu încălca de fapt prea multe legi s-a dovedit a fi deplasată. La patru luni după vizita mea, autorităţile ruse au emis un mandat de arestare pe numele lui în legătură cu un atac informatic masiv lansat împotriva concurentului principal al lui ChronoPay, compania rusească de procesare a plăţilor Assist. Ulterior, Vrublevski a fost arestat, judecat, găsit vinovat şi condamnat la doi ani şi jumătate de închisoare într-o colonie penală

rusească. În mai 2014, după numai un an de la condamnare, a fost eliberat în mod inexplicabil.

În ciuda dezamăgirii mele, întâlnirea cu Vrublevski m-a ajutat să realizez o imagine mai cuprinzătoare a acestui sistem de fraudă – și acesta fusese de fapt scopul meu principal. Discutasem în acest moment cu zeci de cumpărători care contribuiau la perpetuarea problemei spamului și dădusem de urma unora dintre cei mai notorii spammeri din lume. Era momentul să avansez și să intru în tranșee alături de luptătorii antispam pe fronturile acestui război permanent, fără granițe.

# Capitolul 10

# ANTIS

Puține subiecte enervează atât de mult comunitatea spamului și a criminalității informatice cum o fac discuțiile despre „antis" – numele batjocoritor dat de aceasta luptătorilor antispam care acționează singuri sau împreună cu alți *antis* pentru a împiedica sau a elimina operațiunile de e-mail nesolicitat la scară mare care ne invadează. Discuțiile de pe chat purtate între Stupin și sute de expeditori de e-mailuri în masă care au lucrat pentru SpamIt arată că, atunci când nu erau ocupați cu spamul, afiliații își foloseau armatele de boți pentru a ataca off-line pe cineva sau ceva care amenința să le distrugă operațiunile criminale. Foarte adesea, spammeri rivali își îndreptau armele digitale unul împotriva celuilalt. Țintele lor preferate erau însă *antis*, pe care spammerii îi considerau o amenințare reală și prezentă pentru modelele lor de afaceri – și pe bună dreptate.

În trimestrul al treilea al anului 2013, aproape 70% dintre toate e-mailurile expediate zilnic au fost mesaje nesolicitate, transmise în masă prin botneturile de spam. Pentru a vă face o idee despre dimensiunea problemei spamului, vă voi spune că răufăcători precum cei care lucrează pentru SpamIt și alte parteneriate de spam trimiteau *aproximativ 85 de miliarde de e-mailuri nesolicitate în fiecare zi.* Potrivit celor de la InternetWorldStats.com, aproape 2,4 miliarde de persoane foloseau internetul în aprilie 2012, *ceea ce înseamnă că*

*spammerii expediau aproximativ 35 de e-mailuri nesolicitate fiecărui utilizator de internet în fiecare zi.*

Unele dintre tacticile antispam aparţineau unor activişti independenţi, cum ar fi membrii forumului InboxRevenge.com, dedicat demascării spammerilor prin raportarea domeniilor de spam firmelor care rezervă nume de domenii şi prin atragerea atenţiei asupra furnizorilor de găzduire bulletproof toleranţi faţă de spam. Unul dintre cei mai activi membri ai InboxRevenge a fost Adam Drake, acelaşi activist antispam căruia Vrublevski i-a transmis clandestin baza de date SpamIt pentru a-l compromite pe rivalul său Gusev.

Ca o ironie a sorţii, pentru a-i distruge pe spammeri, Drake şi trupa lui de luptători au trebuit să folosească tocmai tehnicile adversarilor. Au creat o serie de instrumente automate menite să plaseze simultan comenzi false de medicamente pe zeci de siteuri promovate prin spam. Aceste programe plasează extrem de repede comenzi de medicamente, utilizând identităţi false şi carduri de credit fictive. Ideea era să se bombardeze bazele de date ale parteneriatelor cu atât de multe mesaje nedorite, încât acestea să fie nevoite să verifice manual fiecare comandă. În unele cazuri, programele respective au încetinit foarte mult funcţionarea siteurilor farmaceutice, blocându-i pe cei interesaţi să facă cumpărături.

„În medie, am expediat zilnic 20 000–30 000 de «comenzi» spre domeniile promovate prin spam", a spus Drake despre iniţiativa lansată în 2007. Drept reacţie, parteneriatele au creat sisteme tot mai sofisticate de detectare a fraudelor care se comportau ca filtrele de spam detestate de ei, dar pentru comenzile false. Aceste sisteme „evaluau" fiecare comandă în ceea ce priveşte probabilitatea de a fi falsă căutând o combinaţie de atribute care corespundea unui risc ridicat. Pe parcursul procesului, spunea Drake, spammerii ajungeau să refuze ori să anuleze multe comenzi de la cumpărători legitimi. „Este evident că i-am făcut să piardă nişte bani."

Sistemele de verificare a comenzilor folosite de SpamIt şi GlavMed semnalau de obicei ca suspecte chiar şi acele comenzi care nu erau prea dubioase. O analiză a arhivei de comenzi sustrasă de la cele două *partnerka* arată că mii de comenzi nu au fost onorate ori au fost respinse din cauza unei infime suspiciuni de fals. De exemplu, multe comenzi au fost refuzate din următorul motiv, care a însoţit mii de comenzi plasate în sistemul SpamIt:

„Această comandă este puţin mai riscantă deoarece numărul de telefon furnizat de utilizator nu este din zona corespunzătoare codului poştal aferent adresei de facturare pentru cardul de credit respectiv."

Potrivit lui Vişnevski – „Vergiliu" al nostru din lumea subterană a spammerilor şi cel care a contribuit la sponsorizarea botnetului de spam Cutwail – măsurile antifraudă au servit, în egală măsură, la a-i ţine sub control pe afiliaţii spam care încercau să genereze vânzări false şi să încaseze comisioane folosind carduri de credit furate. Pe lângă faptul că ar fi determinat plata unor comisioane pentru vânzări fictive, o astfel de activitate frauduloasă ar fi atras, în cele din urmă, o nedorită atenţie asupra sistemelor de procesare a cardurilor de credit ale *partnerka*, care ar fi primit amenzi serioase dacă numărul cererilor de restituire a banilor depăşea un anumit prag (de obicei 1% din numărul total al vânzărilor).

Administratorii SpamIt au luat de asemenea măsuri complexe pentru a se asigura că grupurile şi activiştii antispam nu puteau distruge cu uşurinţă siteurile farmaciilor promovate prin spam. Utilizatorii SpamIt au folosit PC-uri compromise pentru a ascunde adresele reale ale siteurilor farmaceutice, folosind o metodă indirectă denumită găzduire „fast-flux". Această metodă, echivalentul virtual al cunoscutei înşelătorii „alba-neagra", implică schimbarea rapidă a adreselor siteului, astfel încât niciun site să nu fie folosit suficient de mult pentru a fi izolat şi închis.

În cadrul unei configuraţii fast-flux, clientul care accesează un link dintr-un e-mail nesolicitat poate să ajungă pe

alt site sau la altă adresă de internet dacă accesează același link după numai câteva secunde. Clienții potențiali ai acestor farmacii on-line nu vor observa nimic diferit, decât, poate, o scurtă întârziere.

Administratorii SpamIt erau de asemenea foarte atenți la agenții MasterCard, Visa și ai firmelor farmaceutice importante care se ocupă de fraude. Baza de date SpamIt arată că ei adăugau în mod curent aceste adrese de internet și de e-mail la o bază de date a clienților cărora nu li se permitea să plaseze comenzi pe siteurile farmaceutice.

Botmasteri precum Gugle și Cosma făceau în așa fel încât e-mailurile lor să ajungă în inbox și schimbau mereu metodele de lucru pentru a evita noile mijloace de protecție adăugate softwareului și hardwareului antispam. Volumul spamului a devenit atât de copleșitor, încât mulți profesioniști în domeniul securității rețelelor care se ocupau de apărarea rețelelor corporatiste au fost obligați să-și suplimenteze instrumentele antispam bazate pe hardware și software cu „liste negre" de spam (numite și „blocklist").




În esență, o listă neagră de spam conține intervalele de adrese de internet care sunt considerate cel mai adesea surse de spam. În general, adresele de internet de pe listele negre se încadrează în una dintre următoarele două categorii: 1) rețele și furnizori de servicii de internet (ISP) cunoscuți pentru faptul că ignoră spamul din rețelele lor – precum Atrivo și McColo Corp.; 2) PC-uri individuale, infectate cu malware și transformate în „zombie" care distribuie spam.

Cele mai folosite liste negre au fost create de organizații ad-hoc ascunse după nume amuzante, ca Spamhaus, SURBL și URIBL (*BL* vine de la „black list"/lista neagră). Companiile care încearcă să blocheze spamul pentru zeci de mii de angajați încorporează în mod curent aceste liste negre în filtrele de spam, blocând e-mailurile trimise de la oricare dintre adresele de internet listate. Destul de des, rețelele care nu creează spam se pomenesc pe aceste liste negre alături de cei răi.

Majoritatea organizațiilor sunt însă dispuse să accepte faptul că unele e-mailuri legitime nu vor ajunge la destinație dacă astfel se va stopa valul zilnic din ce în ce mai mare al mesajelor nesolicitate.

În ceea ce o privește, comunitatea spammerilor n-a fost deloc amuzată de acești autointitulați gardieni ai conturilor de e-mail și a susținut că ei nu au dreptul să decidă ce e-mailuri ar trebui să primească sau să nu primească utilizatorii internetului. În 2011, o copie a lui Spamdot.biz, un forum foarte discret, frecventat de majoritatea spammerilor de vârf din lume, a fost pusă la dispoziția mai multor autorități și a autorului acestei cărți. Postările de pe forum arată că, încă din 2005, spammerii au început să planifice și să lanseze atacuri la scară mare pe internet, menite să-i pedepsească și să-i intimideze pe activiștii antispam.

Dintre cele mai distructive și agresive campanii de acest fel a făcut parte unul dintre cele mai mari atacuri informatice din istoria internetului, lansat împotriva companiei Blue Security Inc., o firmă antispam tânără și extraordinar de eficientă. Aceasta concepuse o metodă elegantă de stopare a spamului pentru mai bine de 500 000 de utilizatori ai softwareului său Blue Frog. Programul expedia pur și simplu un răspuns rețelei expeditorului, cerându-i spammerului să nu mai trimită utilizatorilor săi e-mailuri nesolicitate.

Dar pentru că aceste solicitări tindeau să fie ignorate, Blue Security a trecut la pasul următor. I-a bombardat pe spammeri cu solicitări din partea tuturor celor 522 000 de clienți ai săi în același timp. Acest lucru a produs o asemenea aglomerare a traficului pe internet, încât spammerii nu au mai putut trimite e-mailuri altor destinatari – un efect devastator, care a determinat câțiva spammeri cunoscuți să dea curs solicitărilor respective.

În scurt timp însă, unii membri importanți ai comunității subterane a spammerilor au declarat că s-au săturat și că era

timpul ca Blue Security să dispară de pe faţa internetului. Potrivit unor lungi discuţii purtate pe Spamdot.biz, cel puţin 12 spammeri de vârf au cheltuit, pe parcursul câtorva săptămâni, peste 15 000 de dolari în încercarea de a-şi uni forţele în vederea declanşării unui atac prin surprindere asupra tuturor clienţilor Blue Security.

Membrii Spamdot descoperiseră că softwareul Blue Frog avea o slăbiciune esenţială: spammerii care acceptau solicitările venite din partea companiei Blue Security primeau un instrument gratuit care le permitea să elimine de pe listele proprii adresele de e-mail ale utilizatorilor Blue Frog. În timp ce Blue Security făcea eforturi să cripteze adresele de e-mail ale utilizatorilor incluse în acel instrument, spammerilor le-a fost uşor să afle care dintre adresele de e-mail de pe listele lor de distribuţie a spamului aparţineau utilizatorilor Blue Frog. Spammerii nu trebuiau decât să compare listele de e-mail nemodificate cu cele curăţate de instrumentul Blue Security. Adresele care lipseau de pe listele de distribuţie curăţate aparţineau utilizatorilor de Blue Security.



Atacul împotriva companiei Blue Security a început cu un e-mail ameninţător, expediat majorităţii celor 522 000 de utilizatori de Blue Frog. Mesajul de mai jos a fost inserat pentru examinare şi ulterior a fost editat de mai mulţi membri ai forumului Spamdot, înainte de a fi trimis prin e-mail utilizatorilor respectivi:

> Ai primit acest e-mail deoarece eşti un utilizator al bine-cunoscutului software „Blue Frog" de la Blue Security.
>
> Astăzi, baza de date Blue Security a devenit cunoscută celor mai periculoşi spammeri din lume. În termen de 48 de ore, baza de date va fi publicată pe internet, iar adresa ta de e-mail va fi cunoscută de toţi. După aceea, vei constata că spamul trimis spre contul tău de e-mail va creşte de 10–20 de ori.
>
> Blue Security îi ataca ilegal pe cei care vând prin e-mail şi a făcut asta cu ajutorul tău. Au fost vizate şi lovite multe siteuri, inclusiv unele care nu generează spam. Programul

Blue Security a fost analizat cu atenție și conține foarte mult malware. Astfel, acesta are capacitatea de a expedia e-mailuri unui număr foarte mare de utilizatori, capacitatea de a ataca siteuri prin atacuri de tip DDoS, capacitatea de a deschide uși ascunse pe orice computer pe care rulează, precum și o funcție ascunsă de autoactualizare a codului, care poate instala orice pe computerul tău și-l poate deschide oricui.

Blue Security menționează ca sediu social o adresă din SUA, dar sediul său principal este la Tel Aviv. Compania este condusă de câțiva evrei ruși, care au fost înainte ei înșiși spammeri. Când își vor termina treaba, ei vor putea să plece, să se ascundă și să-și schimbe identitatea, lăsându-te pe tine să suporți consecințele. NU POȚI SĂ PARTICIPI LA ACTIVITĂȚI ILEGALE și să te aștepți să scapi cu fața curată. Prin acest e-mail ne asigurăm că ești conștient de situație. În curând, vei fi găsit vinovat de infracțiuni informatice precum lansarea de atacuri DDoS asupra siteurilor, conspirație și trimiterea de mesaje nesolicitate pentru tot felul de produse, de la Viagra la pornografie, atât timp cât vei continua să folosești Blue Frog.

Ei nu cer bani pentru descărcarea programului, nu cer bani pentru a elimina e-mailurile de pe listele lor și nu au un flux de venituri vizibil. AU însă 500 000 de computere care le așteaptă următoarea comandă. Ce fac ei acum?

1. Îți utilizează computerul ca să distribuie spam?
2. Îți utilizează computerul ca să atace siteurile concurenței?
3. Fac phishing în fișierele tale pentru a-ți afla identitatea și datele bancare?

Dacă crezi că ajunge să-ți schimbi adresa de e-mail ca să fii în siguranță, dar vei continua să folosești Blue Frog, te așteaptă o mare surpriză. Acesta este doar începutul...

Un membru neobișnuit de activ al forumului Spamdot, utilizatorul cu pseudonimul „BoT", a elaborat un plan diabolic de atac împotriva companiei Blue Security, care avea să întoarcă serviciul antispam al acesteia împotriva utilizatorilor săi. Strategia era simplă și elegantă. Spammerii înregistrau zeci de nume de domenii, care aveau să-i redirecționeze pe vizitatori

spre un singur site controlat de spammeri. După aceea, expediau spam spre toți clienții lui Blue Security și așteptau valul inevitabil de cereri de dezabonare. Când solicitările începeau să sosească la acel unic site, spammerii schimbau pur și simplu setările siteului astfel încât traficul sosit era redirecționat către pagina principală a Blue Security, determinând tehnologia antispam a companiei să se atace pe sine.

„Astfel, ei fie își dau singuri cu stângul în dreptul, fie primesc reclamații de abuz", a explicat BoT într-o postare făcută pe Spamdot chiar înainte de atac. „Și mai bine ar fi ca traficul să fie redirecționat către siteurile CNN, BBC, Reuters și altele similare, care vor începe să scrie că internetul s-a transformat într-un câmp de luptă din cauza «broscuțelor albastre [Blue Frog]»."

La 1 mai 2006, comunitatea spammerilor a declanșat o serie de atacuri tot mai intense asupra serverelor de internet ale firmei Blue Security, împiedicându-i imediat pe utilizatorii legitimi să viziteze siteul acesteia. Blue Security nu fusese încă informată că era vizată, dar reprezentanții companiei știau că clienții întâmpinau dificultăți în accesarea siteului ei. La un moment dat, s-a luat decizia de a redirecționa traficul destinat paginii sale principale, care devenise inaccesibilă, către un blog al companiei, unde a fost postat un mesaj pentru utilizatorii de Blue Frog prin care se recunoștea problema.

Blogul Blue Security era găzduit de un serviciu de blogging administrat de Six Apart Ltd., o companie din San Francisco care administrează milioane de siteuri prin serviciul propriu TypePad. (Six Apart avea să fie ulterior cumpărat de gigantul rus LiveJournal.ru.) Redirecționarea a făcut ca serviciul de blogging Six Apart să sufere cel mai mult din cauza atacului și ca mii de bloguri găzduite de acesta să devină de asemenea inaccesibile. Atacul de tip DDoS a închis, de asemenea, timp de aproximativ 12 ore, operațiunile companiei Tucows Inc., un furnizor de servicii de internet din Toronto care se ocupa de administrarea siteului firmei Blue Security. Elliot Noss, directorul companiei Tucows, a spus că acesta „este de departe cel mai puternic atac

pe care l-am văzut vreodată" şi că doar câteva companii dispuneau de infrastructura necesară pentru a-i rezista, cu atât mai puţin pentru a face faţă unuia mai puternic.

„Acest atac poate fi comparat cu încercarea de a omorî un ţânţar cu o bombă atomică", a spus Noss.

La scurt timp după aceea, Eran Reshef, directorul companiei Blue Security, a primit un e-mail de la unul dintre spammeri, care anterior acceptase să nu mai trimită spam utilizatorilor lui Blue Security şi care l-a informat cum să-l contacteze pe cel care se făcea responsabil de atac.

Mesajul conţinea un link către un site farmaceutic promovat de spammeri în acel moment şi îi cerea lui Reshef să vadă sursa HTML a paginii. Aici avea să găsească un număr ICQ. ICQ (I-Seek-You) era o tehnologie folosită în mesageria instantanee, foarte populară pe atunci în comunitatea infractorilor informatici.

Echipa Blue Security a descărcat o copie a paginii principale a siteului farmaceutic şi apoi a deschis-o într-un editor HTML pentru a se asigura că nu era o capcană cu malware. După aceea, a găsit mesajul ascuns: „privet, stucis v asku 299650295" sau „salut, adaugă ICQ # 299650295."

La scurt timp după ce Reshef a trimis o solicitare de chat către numărul ICQ respectiv, a răspuns cineva care folosea numele „Pharmamaster". Pharmamaster era sarcastic, nefiind deloc interesat să negocieze.

Tue May 02 16:30:57 2006

[16:02] BLUESECURITY: Vrei să negociem acum o soluţie amicală la situaţia actuală? Suntem conştienţi de preocupările voastre, dar, aşa cum ţi-am spus mai devreme şi în pofida a ceea ce crezi, nu vrem să vă afectăm afacerea. Nu suntem o companie antispam obişnuită.

[16:07] PHARMAMASTER: Aţi început cu mine, cu oamenii mei şi cu personalul meu, aşa că o să suferiţi voi mai întâi, ca să ştiţi cine suntem. Iar când o să fiu sigur că aţi priceput cine

suntem, o să putem vorbi. Bluesecurity.com este inaccesibil acum, dar ce-ar fi dacă v-am ține închise toate sistemele vreme de câteva luni?

Reshef a refuzat să discute cu mine despre particularitățile atacului, dar o sursă care a ajutat compania să facă față acestuia a spus că lui Reshef i-a fost amenințată inclusiv familia.

„Atacul a fost atât de îngrozitor, încât țin minte că am fost convocat la o ședință cu Eran și ceilalți, a spus sursa, vorbind sub protecția anonimatului. În plus, era vorba despre un atac personal; Eran primea fotografii ale copiilor lui la un loc de joacă – erau imagini pe care el nu le văzuse niciodată."

Atacurile au continuat mai bine de două săptămâni, cu intensitate crescândă. La un moment dat, atacatorii au început să trimită e-mailuri angajaților de la Blue Security, spunându-le că posedă 70% din baza utilizatorilor de e-mail a companiei Blue Frog și oferind 50 000 de dolari oricărui angajat dispus să le predea restul de 30%.



La 14 mai, conducerea firmei Blue Security s-a întâlnit cu FBI pentru a analiza posibilitățile pe care le avea, dar a fost vorba mai mult despre o formalitate. Două zile mai târziu, Reshef și Blue Security aveau să capituleze. La 17 mai, *Washington Post* a publicat pe prima pagină un articol semnat de autorul acestei cărți, în care se care anunța că Blue Security se recunoscuse înfrântă. Compania primise peste 4 milioane de dolari pentru a ieși din situația creată, dar binefăcătorii ei deciseseră că era momentul să arunce prosopul.

În articol era citat Todd Underwood, pe atunci șef de operațiuni și securitate la firma Renesys Corp., care urmărește calitatea legăturilor la internet. Underwood considera că atacul a fost „previzibil, dar trist".

„Când fondatorii companiei s-au adresat pentru prima oară comunității antispam și i-au întrebat pe membrii acesteia ce credeau despre modelul de afaceri Blue Security, toți le-au spus că era o idee formidabilă și că aceasta va provoca în cele din urmă multe pagube colaterale, a spus Underwood.

Este însă și un fapt foarte regretabil, care ne arată că spammerii sunt cei care câștigă această bătălie."

Cei răspunzători de organizarea atacului asupra companiei Blue Security par să fi fost șefii unuia dintre cele mai mari parteneriate farmaceutice ale momentului. Multe dintre planurile prezentate pe Spamdot.biz cu privire la atacul asupra lui Blue Security au fost formulate și încurajate de un utilizator influent al lui Spamdot.biz, care folosea pseudonimul „Mr. Green". Potrivit celor de la Spamhaus, Mr. Green era un pseudonim folosit de rusul Vlad Hoholkov, un moscovit despre care se spunea că ar fi colaborat cu faimosul spammer Lev Kuvaiev.

Atacul asupra firmei Blue Security a reprezentat un avertisment adresat antispammerilor de pretutindeni. În acel moment, aproape 90% dintre toate mesajele de e-mail erau reclame nesolicitate, iar Blue Security exploatase un sentiment visceral de frustrare existent în rândul utilizatorilor de e-mail, care erau sătui de mesajele pe care le primeau zilnic. Membrii importanți ai Spamdot gestionau însă parteneriate farmaceutice care câștigau lunar milioane de dolari și au văzut în Blue Security avangarda unei noi specii de luptători antispam care reprezentau o amenințare serioasă pentru viitorul afacerilor lor profitabile. Aceștia nu erau dispuși să fie dați la o parte, indiferent de costuri.

Cei de la Spamhaus cred că Hoholkov și Kuvaiev au administrat programele farmaceutice afiliate Mailien și Rx-Partners. Această ipoteză este susținută de convorbirile de pe chat sustrase de la Dmitri Stupin, administratorul lui SpamIt. Într-o conversație din 2008 desfășurată între Stupin și „Joop" – pseudonimul folosit de un rus care se număra printre cei cu câștigurile cele mai mari de la GlavMed – cei doi se referă la un program rival de afiliere numit Affiliate Connection.

„Dacă nu-i un secret, îi cunoști pe Leonid Kuvaiev și Vlad Hoholkov (Mr. Green)?" Fiindcă Stupin a ezitat să răspundă, Joop și-a cerut scuze și a schimbat subiectul. „Îmi retrag

întrebarea. Nu știu ce-a fost în mintea mea. Am uitat că *partnerka* lor a fost Rx-Partners/Stimulcash."

În 2003, Kuvaiev, care era cetățean rus, a fost condamnat pentru încălcarea legilor americane antispam din statul american Massachusetts și obligat să plătească 37 de milioane de dolari pentru botnetul care făcea reclamă unor copii contrafăcute de Microsoft Windows și alte programe de marcă. Se pare că, după aceea, Kuvaiev a fugit din țară ca să nu facă închisoare, dar, la un moment dat, s-a întors în Rusia.

Cei care au râs la urmă au fost totuși cei de la Microsoft. Aceștia i-au plătit pe consultanții companiei rusești Group-IB, care se ocupa cu depistarea infractorilor informatici, să urmărească activitățile lui Kuvaiev și să transmită informațiile autorităților ruse.

În 2011, Kuvaiev a fost arestat sub acuzația de abuz asupra minorilor, iar în prezent se află într-o închisoare rusească. Poliția i-a percheziționat locuința după ce a primit informația că făcea sex cu minore. Acolo, au fost găsite înregistrări video care-l arătau abuzând fete – unele de numai 14 ani – ademenite de la un orfelinat din apropiere. În 2012, Kuvaiev a fost judecat și condamnat pentru abuz asupra minorilor, executând în prezent o pedeapsă de 21 de ani de închisoare (redusă recent la zece ani, potrivit săptămânalului rus *MKRU*).

Contactat prin e-mail, Hoholkov a negat faptul că a fost implicat în atacul contra companiei Blue Security. Nu se știe cine a fost responsabil de organizarea atacului, dar conversațiile de pe chat și discuțiile de pe forumul SpamIt arată clar că Vlad și Lev au acționat ca parteneri și că grupul de spam al lui Kuvaiev a fost puternic implicat.

La scurt timp după atacul împotriva companiei Blue Security, Mr. Green a solicitat administratorilor forumului Spamdot să șteargă toate postările și informațiile despre contul propriu. Unele dintre mesajele lui s-au păstrat însă sub formă de citate în conversațiile de pe forum dintre alți membri ai Spamdot.

Ele arată că Mr. Green a colaborat în planificarea atacului cu un autoproclamat satanist care folosea pseudonimul „Zliden" și avea adresa de e-mail domains@locu.st. Potrivit celor de la Spamhaus, aceasta este ultima adresă de e-mail cunoscută a lui Lev Kuvaiev.

Kuvaiev este considerat unul dintre cei mai aroganți și insensibili spammeri care au existat vreodată. Dar, ca alți maeștri ai e-mailului de masă, a avut grijă să-și separe diversele identități on-line de existența off-line, schimbând adrese de e-mail și pseudonime și ștergând frecvent postările vechi pentru a-i păcăli pe vânătorii de infractori informatici și pe activiștii antispam.

Chiar și așa, experiența lui Kuvaiev (și cea a contemporanilor săi, precum Cosma și Nechivolod) arată că, deși internetul poate pierde uneori urma identităților on-line, activiștii antispam și cei care luptă pentru securitatea internetului au o memorie mult mai lungă și sunt dispuși să-și dea toată osteneala pentru a-i aduce pe spammeri în fața justiției.




## SPAMHAUS SUB ASEDIU

Membrii forumului Spamdot.biz au planificat și au executat de asemenea câteva atacuri puternice împotriva organizației Spamhaus, ca și asupra URIBL și SURBL, care întocmesc și actualizează liste negre de spam utilizate pe scară largă. În octombrie 2008, „Ika", administratorul lui Spamdot, a postat pe forum un mesaj cu privire la campania de strângere de fonduri de la spammeri în vederea lansării unui atac DDoS de durată împotriva siteurilor celor trei furnizori de liste negre.

Mesajul suna cam așa:

> Stimați domni,
>
> Am strâns peste 3 000 de dolari; o parte din sumă va fi folosită în primele patru zile de DDoS împotriva lui URIBL și Spamhaus. De asemenea, am cumpărat instalări de boți în

valoare de 1 000 de dolari, la un tarif de 25 de dolari pentru 1 000 de boți.

Țintele acestui DDoS: 1) infrastructura lists.uribl.com/; 2) bazele afacerilor lui Linford [fondatorul lui Spamhaus] – www.uxn.com și www.ultradesign.com/net, unde se află baza de date de rezervă Spamhaus; 3) ambele fețe ale Spamhaus.org.

Un reprezentant al parteneriatului farmaceutic on-line Affiliate Connection a spus că spammerii săi puteau folosi câteva milioane de PC-uri compromise într-un atac masiv asupra lui Spamhaus. După părerea lui însă, costurile de oportunitate ale unui asemenea atac erau ridicate, deoarece companiile antiabuz puteau să identifice rapid și să treacă pe lista neagră toate mesajele ulterioare (inclusiv spamul care avea să aducă bani) de la zombii de spam. În plus, liderul Affiliate Connection a spus că URIBL și SURBL achiziționaseră recent, de la un furnizor specializat important, servicii de protecție împotriva atacurilor DDoS.





Administratorii SpamIt au răspuns că măsurile respective nu erau nici pe departe suficiente pentru a-i face să renunțe la planurile lor.

„Perfect atunci, a declarat Ika, dacă ei au canale anti-DDoS puternice, va trebui să acționăm în forță și hotărât pentru a le umple țevile. Vor trebui să facă față unui trafic uriaș, ceea ce va fi o problemă reală pentru ei. Va fi scump, dar cred că unii afiliați pot aloca câteva sute de dolari pe zi."

După câteva săptămâni, discuțiile de pe Spamdot.biz privind planurile de atac împotriva lui Spamhaus generaseră pagini întregi de postări, dar puțină acțiune. Dezgustat de colegii săi, GeRa – afiliatul SpamIt și Rx-Promotion care opera botnetul de spam Grum – i-a îndemnat pe alți spammeri să facă sacrificii pentru binele industriei.

Fac apel la spammerii cei mai importanți: câștigați lunar din comisioane între 50 000 și 200 000 de dolari, nu puteți găsi 3 000 de dolari ca să rezolvăm problema asta?

Docent, administratorul botnetului de spam Mega-D, a răspuns că el și echipa lui erau gata să împrumute bani pentru un atac susținut împotriva Spamhaus. Curând însă, discuția s-a împotmolit când a trebuit să se decidă cine avea să-și asume responsabilitatea pentru conducerea și organizarea atacului.

Colac peste pupăză, nu toți membrii forumului sprijineau atacul contra lui Spamhaus și a celorlalți furnizori de liste negre. Severa, cel care a creat și a gestionat botneturile de spam Waledac și Storm, a avut o atitudine mai filosofică, observând că „Spamhaus este doar o parte a unui uriaș proces de evoluție" și că filtrele de spam au ajutat de fapt la separarea spammerilor începători de profesioniști și îi descurajează pe potențialii spammeri lipsiți de experiență să se apuce de această meserie.

„Băieți, noi NU MAI PUTEM trăi fără filtre de spam", a explicat el într-un răspuns la discuția despre Spamdot. Pledând pentru utilizarea continuă, pe scară largă a filtrelor de spam, comentariile lui Severa trebuie să li se fi părut aproape o erezie multora dintre colegii săi. Acest baron al spamului și-a dat însă bine seama că spammerii neexperimentați erau o pacoste pentru industrie și că aceștia îi diminuau profiturile. Dacă filtrele de spam reușeau doar să-i țină la distanță pe micii profitori, atunci așa trebuia să fie.

„De fapt, ele îi opresc pe începători și nepricepuți. Imaginați-vă ce s-ar întâmpla dacă toate filtrele ar fi oprite în clipa asta. Ați mai câștiga bani? NU! E-mailul ar dispărea ca serviciu de comunicare, atât și nimic mai mult. Spamhaus nu e bun sau rău; Spamhaus este Spamhaus și atât."

„Swank", un membru al Spamdot, a spus că, în general, era de acord cu afirmația lui Severa, dar Spamhaus trebuia să fie umilit.

„Severa, ai făcut o observație foarte bună și ai perfectă dreptate", a scris el. „Filtrele de spam și multe altele sunt bune pentru tehnologie și internet deoarece ambele părți – spammerii și cei antispam – se adaptează mereu și schimbă lucrurile din

jur, pentru a o lua înaintea celuilalt. Rezultatul final este acela că tehnologia se îmbunătățește constant, ceea ce, după cum ai spus, îi ține pe profesioniști în viață și îi elimină pe novici. Acestea fiind spuse, companii stupide ca Spamhaus nu sunt corecte cu spammerii docili. Spamhaus abuzează de puterea pe care o are pentru a elimina pe ORICE spammer, indiferent dacă persoana respectivă este sau nu este docilă. Spamhaus îi urăște pe toți cei care vând prin e-mail. Asta e o prostie absolută. Așa ceva nu e corect pentru nimeni. Spamhaus trebuie să înțeleagă că ei nu sunt de neatins și își vor da seama curând de asta."

În octombrie 2008, GeRa i-a anunțat pe membrii Spamdot că va lansa un instrument de atac automat pe care programatorii săi îl realizaseră pentru a ajuta comunitatea să participe la un atac masiv asupra organizației Spamhaus. Programul, numit Anti-Haus v. 1.0, a fost distribuit principalilor proprietari de botneturi, care, la rândul lor, l-au instalat pe zeci de mii de PC-uri compromise, pe care le controlau și care distribuiau deja spam.

Un reprezentant al Spamhaus, care s-a identificat doar ca „Barry", a declarat că organizația nu-și amintește de atacul din octombrie 2008, spunând că Spamhaus a pierdut șirul atacurilor puternice lansate asupra sa de-a lungul anilor.

În martie 2013, Spamhaus a fost supusă unui atac pe care nu avea să-l uite prea curând. De fapt, unii experți l-au considerat cel mai mare atac informatic concertat care a avut loc vreodată pe internet. Un grup de furnizori de găzduire bulletproof, uniți sub titulatura „Stophaus", au decis să atace furnizorul antispam. Stophaus a creat un forum on-line pentru a coordona atacul după ce Spamhaus a inclus pe lista sa neagră un anumit furnizor de găzduire bulletproof: o rețea cunoscută sub denumirea de CB3ROB sau „Cyberbunker", deoarece opera dintr-un buncăr NATO puternic fortificat din Olanda.

Atacatori aliați cu Stophaus au lansat un asediu digital de nouă zile, în timpul căruia siteul organizației Spamhaus

a fost bombardat cu până la 300 de miliarde de megaocteți de date pe secundă. După cum afirmau cei de la *New York Times*, „jetul" de date îndreptat spre Spamhaus nu numai că l-a doborât pe furnizorul antispam, ci a afectat și rețelele vecine, astfel încât, potrivit celor de la CloudFlare, rețeaua de distribuție de conținut a organizației, sute de milioane de oameni au constatat că mesajele lor erau expediate cu întârziere sau nu erau expediate deloc.

Când atacatorii aliați cu Stophaus și-au dat seama că nu vor putea doborî CloudFlare, pe care Spamhaus o angajase spre a o proteja de atacurile DDoS, au început să bombardeze „punctele de peering", în care rețelele de internet fac schimb de trafic, inclusiv pe cele de la Londra, Amsterdam, Frankfurt și Hong Kong.

*New York Times* a anunțat că autoritățile din Spania l-au arestat ulterior pe Sven Olaf Kamphuis, un olandez de 35 de ani, considerat responsabil de coordonarea atacului fără precedent lansat asupra lui Spamhaus. Potrivit celor de la Spamhaus și informațiilor din mass-media, Kamphuis a susținut că el era propriul lui stat independent în Republica Cyberbunker. *Guardian* a anunțat că Kamphuis a fost extrădat în Olanda, dar nu există niciun indiciu că el ar fi fost urmărit penal acolo. Kamphuis nu recunoaște că a fost implicat în atac și a spus că nu a făcut decât să țină legătura cu presa pentru CB3ROB/Cyberbunker.

Atacul celor de la Stophaus a fost ultimul și cel mai puternic avertisment cu privire la faptul că, în prezent, astfel de arme de perturbare în masă a traficului sunt ușor de obținut de orice persoană sau organizație care vrea să le folosească. În atacul asupra Spamhaus – numit atac de reflectare și amplificare a DNS-urilor – s-au folosit servere de nume de domeniu (DNS) negestionate de pe web pentru a se crea un volum imens de trafic cu scopul de a intimida și de a reduce la tăcere țintele.

Pentru a înțelege ce se întâmplă, voi da câteva explicații tehnice. Serverele DNS funcționează ca paginile albe ale internetului, „rezolvând" sau transformând nume de domenii ușor de

reținut de către oameni, cum ar fi exemplu.com, în adrese numerice de rețea utilizate de computere. În mod obișnuit, serverele DNS furnizează servicii numai computerelor dintr-un domeniu de încredere, în acest caz exemplu.com. Atacurile de reflectare a DNS-urilor se bazează însă pe routere de internet ale unor persoane fizice și juridice care sunt configurate să accepte interogări sosite de oriunde de pe web. Atacatorii pot trimite interogări DNS false la aceste servere așa-numite „deschis recursive", falsificând interogarea astfel încât să pară că provine din rețeaua țintei. Astfel, atunci când răspund, serverele DNS fac acest lucru la adresa falsă (a țintei).

Componenta de amplificare a atacului se bazează pe capacitatea de a realiza interogări DNS astfel încât răspunsurile să fie mult mai mari decât cererile. Acest lucru se face prin exploatarea unei extensii a standardului DNS care permite transmiterea de mesaje DNS mari. De exemplu, un atacator poate formula o cerere DNS de mai puțin de 100 de octeți, care să determine un răspuns de 60–70 de ori mai mare. Acest efect de amplificare este extrem de pronunțat dacă atacatorii interoghează simultan zeci de servere DNS cu cereri false.



Vestea bună este că experții în securitate și internet au înțeles de mult cum pot să blocheze aceste atacuri extraordinar de puternice. „Câțiva specialiști în securitatea computerelor au subliniat că atacurile ar fi fost imposibile dacă marile firme de internet din lume s-ar fi asigurat pur și simplu că pachetele de date erau cu adevărat expediate de clienții lor, nu de botneturi", au scris John Markoff și Nicole Perlroth de la *New York Times*.

Vestea proastă este că puține lucruri s-au schimbat de la apariția acestor atacuri cu peste un deceniu în urmă, spunea Rodney Joffe, vicepreședinte și tehnolog principal la Neustar, o companie de securitate care îi ajută pe clienți să facă față unor atacuri on-line uriașe. Joffe estimează că există aproximativ 25 de milioane de routere aparținând unor persoane fizice și juridice greșit configurate sau vechi, care pot fi exploatate în

aceste asedii digitale. Cele mai multe dintre ele sunt routere de uz casnic furnizate de ISP-uri sau routere comerciale greșit configurate. Foarte multe dispozitive se află la ISP-uri din țări în curs de dezvoltare sau la furnizori de internet care nu văd niciun avantaj în a cheltui bani pentru binele internetului.

„În aproape toate cazurile, este vorba despre o opțiune care poate fi configurată de ISP, dar trebuie să-l determini să facă asta, a spus Joffe. Mulți asemenea furnizori au profituri foarte mici și n-au niciun interes să-și protejeze utilizatorii finali – și, de altfel, pe restul utilizatorilor de Internet."

Iar aici este problema. Nu cu mult timp în urmă, dacă un spammer sau un hacker dorea să lanseze un atac masiv pe internet, trebuia să asambleze un botnet imens format din foarte multe PC-uri compromise. În prezent, un asemenea atacator n-are nevoie de o asemenea armată imensă de boți. Înarmați cu doar câteva sute de PC-uri infectate de boți, spunea Joffe, atacatorii de azi pot elimina aproape orice țintă de pe internet, grație milioanelor de routere de internet greșit configurate care pot fi mobilizate în orice clipă pentru atac.

„Dacă băieții răi lansează un atac, pot începe prin a utiliza 20 000 de asemenea routere greșit configurate, iar dacă ținta mai este on-line, numărul lor va crește la 50 000, spunea Joffe. În majoritatea cazurilor, ajung 100 000 pentru a scoate din funcțiune cele mai mari siteuri, dar există 25 de milioane de asemenea routere disponibile."

# Capitolul 11

# ÎNCHIDERILE

La nouă luni după călătoria făcută în Rusia pentru a-l întâlni pe Vrublevski, priveam din nou cerul înstelat al nopții, de pe puntea altei nave mari, într-o țară străină. De data aceasta, mă aflam pe un pachebot vechi, ancorat în portul Rotterdam.

De cealaltă parte a hublourilor cu geamuri înghețate, o orchestră cânta la o recepție dată în cinstea participanților la conferința de securitate informatică GovCert, la care susținusem, în cursul zilei, o prezentare despre războiul dintre Gusev și Vrublevski. Era foarte frig, vântul bătea cu putere, iar eu așteptam să le fiu prezentat anchetatorilor de la Serviciul Federal de Securitate din Rusia (FSB). Câțiva agenți FSB care participau la conferință le spuseseră gazdelor noastre olandeze că doreau să mă cunoască, dar numai într-un cadru privat.

Mâinile îmi înghețaseră atât de rău, încât nu mai puteam să țin paharul de bere, care era acoperit cu un strat subțire de gheață. L-am așezat pe pervaz și, tocmai atunci, am auzit scârțâitul puternic al ușii groase din oțel care se deschidea înapoia mea. Pe punte își făcu apariția una dintre organizatoarele conferinței. Aceasta i-a prezentat pe cei trei bărbați care veneau după ea, apoi s-a grăbit să se întoarcă înăuntru, la căldură.

Un bărbat îndesat, de vârstă mijlocie, care îmi fusese prezentat ca ofițerul cel mai mare în grad, vorbea în rusă, în timp ce un domn mai tânăr traducea în engleză, trăgând, când se

întrerupea, dintr-o țigară Marlboro. M-au întrebat dacă știam ceva despre compania moscovită Onelia. Am spus că nu, i-am rugat să-mi zică numele pe litere și am întrebat de ce-i interesa. Superiorul a spus că, după părerea lor, aceasta era implicată în procesarea plăților pentru diverse afaceri din domeniul criminalității informatice.

Mai târziu, întors în camera mea de hotel, am căutat on-line detalii despre companie, dar n-am găsit nimic. M-am gândit să întreb câteva dintre cele mai bune surse ale mele din Rusia ce știau despre Onelia, însă ceva mi-a spus că era posibil ca agenții FSB să fi sperat că eu voi face exact asta. Ar fi putut după aceea să-mi afle sursele când acestea începeau să se intereseze de o firmă misterioasă (și probabil fictivă) numită Onelia.

Paranoia m-a biruit și am uitat de acele informații. Asta până când, câteva luni mai târziu, am descoperit că Onelia (care se pare că se pronunță mai degrabă Oneliia) era numele societății cu răspundere limitată aflate în spatele siteului Gateline.net, care a procesat zeci de mii de tranzacții ale clienților cu SpamIt și Rx-Promotion.

Cei de la Gateline.net afirmă că serviciile companiei sunt folosite de firme din diverse domenii, inclusiv turism, vânzarea biletelor de avion, telefonie mobilă și tranzacții în monede virtuale. Dar, conform datelor cu privire la plăți și afiliați sustrase de la SpamIt și Rx-Promotion, Gateline a procesat de asemenea majoritatea cumpărăturilor făcute pe siteuri farmaceutice ilicite promovate de spammerii care lucrează pentru cele două programe.

Legătura dintre Gateline și programele de spam este confirmată de jurnalele de chat confiscate în 2011 de anchetatorii ruși care cercetau activitatea SpamIt. În ele există sute de conversații purtate între Dmitri „SaintD" Stupin, coproprietarul SpamIt, și Nikolai Victorovici Illin, un administrator al Gateline care folosea pseudonimul „Șaman" (shaman@gateline.net) și care era numit „Nikolai" sau „Kolea", diminutivul

numelui respectiv. Jurnalele conţin peste 200 de conversaţii purtate între Şaman şi Stupin în perioada 2007–2010.

Discuţiile avute de Stupin arată că Şaman avea o influenţă enormă asupra operaţiunilor cotidiene ale SpamIt. Reţeaua avea dificultăţi majore în a le oferi cumpărătorilor capacitatea de a folosi pentru plată serviciile MasterCard, în special deoarece compania MasterCard pare să fi fost mult mai vigilentă decât Visa în privinţa folosirii serviciilor sale de către farmaciile on-line ilicite. Datele cu privire la plăţi ale SpamIt indică faptul că Şaman primea o cotă considerabilă (aproximativ 8%) din toate vânzările procesate de farmaciile SpamIt şi că, uneori, primea zeci de mii de dolari pe săptămână pentru serviciile sale.

În conversaţia care urmează, desfăşurată între Şaman şi Stupin la 23 noiembrie 2009, primul îl mustră pe Stupin fiindcă n-a fost mai atent la tranzacţiile care, credeau ei, fuseseră făcute sub acoperire de agenţii antifraudă ai MasterCard. La începutul conversaţiei, Şaman postează un link spre un articol despre ancheta penală iniţiată de anchetatorii ruşi în cazul SpamIt şi al lui Igor Gusev, partenerul lui Stupin.

ŞAMAN: www.runewsweek.ru/country/31283/

STUPIN: Da, da.

ŞAMAN: Ţi-aş sugera să nu faci prea multă reclamă (PR) băncilor.

STUPIN: Este ultimul lucru de care avem nevoie.

ŞAMAN: Altminteri, toată afacerea se va prăbuşi. A mai existat deja ceva de genul ăsta.

STUPIN: Igor încearcă să elimine postările alea.

ŞAMAN: Bine. Care-i treaba cu războiul informaţiilor? Trebuie să oprim chestia asta într-un fel. O să distrugeţi toată afacerea.

STUPIN: Noi??? N-a existat nici măcar o postare a noastră. Igor le scoate tot timpul. Noi nu facem nimic altceva.

ŞAMAN: Nu-i mai răspundeţi postărilor de pe forum şi RedEye se va linişti.

STUPIN: O să-l întreb pe Igor dacă a răspuns. Dacă a făcut-o, o să-i cer să n-o mai facă.

ŞAMAN: [Indicând o adresă de e-mail care se pare că aparţinea unui agent antifraudă de la MasterCard] Termină-l pe nenorocitul ăsta – e de la MasterCard. A făcut o achiziţie. www.iacva.org/PDF/William%20Hanlin.pdf

ŞAMAN: Fii mai atent cu lotul. Termină-i şi pe ăştia: Charles Wilson, Stephen Carpenter, Fredric Manger, Sandro Racheli...

ŞAMAN: Ce-i cu tine?

STUPIN: Programatorii noştri verifică ce s-a întâmplat. Aşa ceva n-ar trebui să se întâmple.

Când m-am întâlnit cu ofiţerii FSB, laţul începuse deja să se strângă în jurul lui Vrublevski, iar Gusev închisese de mult SpamIt şi părăsise efectiv pe furiş GlavMed. Acum se părea că FSB viza infrastructura financiară care deservea atât parteneriatele farmaceutice concurente, cât şi alte programe de farmacii on-line ilicite.





Războiul farma dintre Vrublevski şi Gusev a fost extrem de costisitor pentru industria spamului, iar conflictul lor i-a afectat din plin pe toţi cei din domeniu. În prezent, cei doi sunt înjuraţi pe mai toate forumurile dedicate criminalităţii informatice pentru că i-au lipsit pe spammeri de profituri de zeci de milioane de dolari şi pentru că au atras atenţia autorităţilor şi experţilor în securitate asupra spammerilor.

„Idioţii ăştia doi au distrus afacerea cu spam, a spus Vişnevski într-o discuţie din mai 2012. Pentru cei mai mulţi, ea n-a fost oricum niciodată foarte profitabilă; poate cincizecebăieţi să fi câştigat bani frumoşi din spam. Dar după ce Pavel şi Gusev au pornit războiul dintre ei, toţi au început să creadă că fiecare spammer este un milionar şi să umble după spam şi spammeri."

Vişnevski s-a plâns că, deoarece veniturile obţinute din afacerea lui cu spam au scăzut, a fost obligat să-şi ia un al doilea serviciu, legal sau „alb", pentru a-şi completa câştigurile „negre". El continuă să vândă multor altor spammeri programul

pe care-l folosește la spam, dar lucrează și ca administrator de sistem al unei companii din Moscova, fiind plătit în esență pentru a o apăra de unele dintre amenințările la care el însuși contribuie cu afacerea lui cu spam.

E limpede însă că afacerea respectivă este în regres după epoca de aur de dinainte și de după McColo. Aceasta se datorează nu atât faptului că distribuirea spamului a devenit o activitate mai periculoasă în Rusia, cât faptului că Vișnevski are probleme cu atragerea și păstrarea programatorilor talentați, în stare să-l ajute să ducă afacerea mai departe. Programatorii talentați din Moscova pot lucra legal la firme de înaltă tehnologie, pe salarii mari, iar mulți dintre cei care i-au fost mult timp angajați au plecat la companii legale din tânărul, dar promițătorul domeniu al tehnologiei de vârf de la Moscova.

„Mulți reprezentanți ai lumii subterane nu pot găsi acum programatori buni deoarece salariile pe care ei le primesc la Moscova sunt mult mai mari decât se poate câștiga din spam, spunea Vișnevski. Afacerea asta s-a dus naibii când a fost arestat Pașa [Vrublevski]. Dacă Pașa și Gusev n-ar fi declanșat războiul ăla prostesc, toată lumea ar fi fost mult mai fericită."

Criticile lui, deși aspre, nu sunt deloc exagerate. Într-adevăr, industria spamului a fost serios afectată în ultimii ani. Înainte de închiderea SpamIt în octombrie 2010, volumul de spam expediat zilnic pe plan mondial se ridica la aproximativ 5,5 miliarde de mesaje. După închiderea SpamIt, volumul de spam global expediat zilnic a înregistrat un declin însemnat. Potrivit celor de la Symantec, în martie 2011, volumul de spam scăzuse la puțin peste un miliard de mesaje zilnic, iar, de atunci, el s-a menținut în jurul acestui nivel.

Spamul rămâne o problemă majoră, dar s-a adâncit și mai mult în subteran, iar jucătorii mari par să fie mai circumspecți în activitățile lor. Desigur, războiul dintre Gusev și Vrublevski a fost doar unul dintre factorii care au contribuit la declinul economiei bazate pe spam, chiar dacă a fost considerabil. Dacă industria spamului a devenit mai puțin atractivă pentru

potențialii răufăcători informatici, acest lucru poate avea legătură cu închiderea în ultimii ani a unor mari botneturi de spam.

Iată alte câteva închideri notabile care au vizat operatori de botneturi și mașinile lor infracționale:

• În mai 2009, Comisia Federală pentru Comerț a convins un tribunal să-i oblige pe furnizorii de internet să nu mai direcționeze traficul pentru 3FN, un furnizor de găzduire din California de Nord identificat de anchetatori și comisie drept sursă majoră de conținut on-line dăunător. Forumul lui Vrublevski, Crutop.nu, era găzduit de acesta și a fost obligat să-și găsească altă casă după închiderea 3FN.

• În noiembrie 2009, firma de securitate FireEye din Milpitas, California, a dus o campanie coordonată de eliminare a botnetului Mega-D. Un an mai târziu, presupusul proprietar al Mega-D, Oleg „Docent" Nikolaenko, în vârstă de 24 de ani, a fost arestat în Las Vegas. Acesta a pledat vinovat în 2013 de răspândirea de malware în computere protejate și a primit o condamnare echivalentă cu timpul petrecut deja în închisoare, plus trei ani cu suspendare. (Nikolaenko stătuse deja douăzeci și șapte de luni în detenție înainte de a fi judecat.)

• În ianuarie 2010, angajați ai firmei de infrastructură de internet Neustar au preluat controlul asupra botnetului de spam Lethic, o rețea ilegală de difuzare a spamului compusă din peste 200 000 de PC-uri infectate.

• În februarie 2010, Microsoft a anunțat prima dintr-o serie de închideri dictate de instanță ale unor botneturi de spam importante. Prima țintă a fost botnetul de spam Waledac al lui Severa, care, în acel moment, expedia zilnic miliarde de e-mailuri nesolicitate prin intermediul unei rețele de peste 60 000 de computere compromise. În demersul făcut, Microsoft a convins un tribunal federal american să-i acorde dreptul de a intra legal în posesia a 277 de domenii de internet pe care botmasterul lui Waledac le folosea pentru a-și controla imperiul.

• În octombrie 2010, autoritățile armene l-au arestat pe rusul Gheorghi Avanesov, de 27 de ani, închizând în același timp botnetul Bredolab, un motor de spam care deturnase milioane de PC-uri de când începuse să funcționeze în 2009. Experții spun că, în perioada sa cea mai bună, Bredolab expedia zilnic peste trei miliarde de mesaje. Anchetatorii au afirmat că Avanesov câștiga lunar peste 130 000 de dolari închiriind botnetul altor spammeri. Potrivit unui reportaj BBC, Avanesov a fost judecat ulterior pentru sabotaj informatic și condamnat la patru ani de închisoare în Armenia. Arhivele SpamIt indică faptul că el avea mai multe profiluri afiliate care-i aduceau venituri de la respectivul program farmaceutic.

• În martie 2011, Microsoft a pus ochii pe Rustock, lansând în ascuns un atac prin intermediul sistemului judiciar american, cu scopul de a prelua controlul asupra domeniilor folosite pentru a controla motorul de spam al lui Cosma. În acel moment, se estima că Rustock rula pe 815 000 de computere și expedia zilnic un volum imens de e-mail nesolicitat. În acest caz, Microsoft a primit ajutor din partea producătorului de medicamente Pfizer, ale cărui produse și mărci comerciale apăreau cel mai des în mesajele înșelătoare difuzate de spammeri.

• În iulie 2011, Microsoft a anunțat că oferă o recompensă de 250 000 de dolari pentru informații care să ducă la arestarea și condamnarea botmasterului Rustock. Interesant este că, deși Spamdot.biz și-a închis porțile după ce Gusev a fost numit, în octombrie 2010, „spammerul numărul unu al lumii" de către autoritățile rusești, forumul respectiv n-a dispărut. Și-a schimbat doar numele și adresa. La scurt timp după ce Microsoft a oferit acea recompensă, Cosma, administratorul lui Rustock (care-și schimbase deja pseudonimul în „Tarelka", adică „farfurie" în limba rusă), a putut fi văzut pe noul forum cerând sfaturi despre obținerea unui pașaport nou sub un nume fals.

• În iulie 2012, FireEye și Spamhaus au pus ochii pe botnetul Grum, care era printre primele trei cele mai active mașini

de spam, expediind zilnic 18 miliarde de mesaje. Închiderea realizată în urma colaborării lor a redus în scurt timp volumul global de spam, dar codul-sursă pentru Grum a căzut ulterior în mâinile altor răufăcători, determinând renașterea sa. Grum rămâne activ și în ziua de azi.

• În iulie 2013, Microsoft și FBI au anunțat o operațiune comună în urma căreia au fost închise peste 1 400 de botneturi ce foloseau malwareul Citadel pentru a controla PC-uri infectate. Citadel a fost folosit în primul rând de grupări criminale care se ocupau cu golirea conturilor bancare prin intermediul tâlhăriilor on-line.

• În decembrie 2013, Microsoft a colaborat din nou cu FBI și cu autoritățile din Europa pentru a întrerupe funcționarea botnetului ZeroAccess. Acesta a fost deseori asociat cu alte amenințări (inclusiv botneturi de spam și antiviruși falși), dar a fost conceput în special pentru a deturna rezultatele motoarelor de căutare de pe PC-urile infectate și pentru a-i redirecționa pe utilizatori către siteuri ce taxau în mod fraudulos firmele pentru publicitatea on-line.



• În iunie 2014, FBI, în colaborare cu mai mulți parteneri internaționali și firme de securitate private, a închis botnetul „Gameover Zeus", o rețea cu peste un milion de computere compromise. De asemenea, FBI l-a numit pe rusul Evgheni Mihailovici Bogacev, de 31 de ani, creierul din spatele operațiunii respective și principalul autor al botnetului. Potrivit Departamentului de Justiție din SUA, botnetul Gameover a fost folosit pentru a fura peste 100 de milioane de dolari de la firmele care i-au căzut victimă. Botnetul a fost, de asemenea, o platformă importantă pentru lansarea unor acțiuni on-line costisitoare de șantajare a utilizatorilor individuali de computere.

Dar nu numai industria spamului a avut de suferit temporar din cauza războiului dintre Gusev și Vrublevski. ChronoPay era profund implicată în procesarea plăților pentru

parteneriate care promovau produse antivirus dubioase, iar atunci când Vrublevski a devenit obiectul unei anchete penale în 2011, rețelele sale s-au prăbușit. Practic peste noapte, rețelele care promovau antiviruși dubioși n-au mai funcționat pentru că au pierdut conexiunea cu rețelele de carduri de credit. Vrublevski a fost arestat la sfârșitul lunii mai a anului 2011 pentru fapte de altă natură, iar, în august 2011, cei de la firma de securitate informatică McAfee au observat o scădere cu 60% a numărului utilizatorilor care raportau probleme cu programele antivirus contrafăcute.

## ÎNCHIDEREA DOMENIILOR ȘI CURĂȚAREA MOTOARELOR DE CĂUTARE

Un alt front în războiul împotriva spamului a vizat siteurile farmaciilor promovate prin e-mailuri nesolicitate. De regulă, spammerii căutau să apeleze la administratori de nume de domeniu care să-i ignore pe cei ce înregistrau lunar sute sau chiar mii de domenii care urmau a fi utilizate în campanii de spam farmaceutic. Multă vreme, unii dintre cei mai mari jucători din sectorul numelor de siteuri au refuzat solicitările grupărilor antispam de a anula înregistrarea unor domenii care fuseseră în mod clar create pentru a obține beneficii de pe urma spamului.

John Horton, fost adjunct al șefului Biroului de politici în domeniul antidrog de la Casa Albă, actualmente, președinte al LegitScript, o firmă care se ocupă cu verificarea farmaciilor de pe internet, urmărea de mulți ani ce se întâmpla cu domeniile farmaciilor ilicite. Horton a spus că, de la o vreme, majoritatea administratorilor de nume de domenii susțineau că nu e de datoria lor să cerceteze modul în care își folosesc domeniile clienții lor.

Situația a început să se schimbe la sfârșitul anului 2008, când companiei estoniene EstDomains – un administrator

de nume de domenii care devenise în mod evident preferatul spammerilor și escrocilor de pe internet – i-a fost revocată acreditarea de către Internet Corporation for Assigned Names and Numbers (ICANN), organizația nonprofit care supraveghează sectorul înregistrării numelor de domeniu. ICANN a luat măsuri după apariția în *Washington Post* a unui articol semnat de autorul acestei cărți, care constata că directorul general al companiei EstDomains – afaceristul estonian Vladimir Țastin – fusese condamnat anterior pentru spălare de bani, fals și fraudă cu carduri de credit.

ICANN a acționat după ce, în articolul meu din *Washington Post*, am atras atenția asupra unei clauze puțin cunoscute din contractele pe care administratorii de nume de domeniu ca EstDomains le semnau cu ICANN, potrivit căreia administratorii nu aveau voie să numească directori cu cazier. Așa cum am menționat în capitolul 8, Țastin fusese unul dintre primii investitori importanți ai ChronoPay, iar, în 2011, fusese arestat în Estonia împreună cu alte șase persoane acuzate de gestionarea unui botnet enorm, care cuprindea peste patru milioane de PC-uri din toată lumea.



Horton a spus că incidentul cu EstDomains i-a speriat pe mulți dintre cei care își desfășurau activitatea în sectorul înregistrării domeniilor. Unul dintre partenerii cei mai apropiați ai lui EstDomains era o firmă indiană Directi, care se lupta și ea cu un val de reclamații privind abuzurile spammerilor care foloseau serviciul său.

„Cu trei–patru ani în urmă, nimeni nu suspenda nume de domenii implicate în activități farmaceutice dubioase pe internet, cu excepția cazului în care puteai să dovedești fără putință de tăgadă că domeniile respective obțineau beneficii de pe urma activităților de spam, spunea Horton. Directi a fost unul dintre primii administratori de nume de domenii care au spus că, dacă știu că siteurile vând fără rețetă medicamente eliberate doar pe bază de rețetă și că [acele medicamente]

sunt expediate într-o altă țară, încălcând legile țării respective, vor lua măsuri pentru a suspenda domeniul. După aceea, am văzut că GoDaddy, eNom și alții procedează la fel. Dacă se ia în considerare cota de piață a administratorilor de nume de domenii, se constată că aproximativ 60–70% dintre aceștia iau măsuri [de suspendare a domeniilor] în baza acelor acuzații."

Dacă membrii comunității internetului nu erau conștienți de riscurile financiare pe care le presupune o implicare prea mare în rețeaua de siteuri farmaceutice, mesajul primit de ei în august 2011 a fost foarte clar. Departamentul de Justiție al SUA a anunțat atunci că Google a acceptat să plătească o amendă de 500 de milioane de dolari pentru a pune capăt unei anchete penale în care era acuzat că permisese unor presupuse farmacii canadiene – inclusiv mai multor farmacii on-line ilicite – să facă publicitate unor medicamente distribuite în SUA. Suma de 500 de milioane de dolari trebuia să reprezinte venitul obținut de Google din publicitate de la farmaciile canadiene și venitul obținut de aceste farmacii de la clienții americani care cumpărau medicamente supuse unor restricții.



## VISA STRÂNGE ȘURUBUL

Probabil că, în ultimii doi ani, impactul cel mai durabil asupra economiei spamului l-a avut un studiu dat publicității de un grup de cercetători care a realizat un plan al rețelelor de spălare a banilor pe care se bazau aproape toate parteneriatele farmaceutice. Mai important, cercetătorii au reușit să folosească propriile constatări pentru a forța firme renumite să exercite presiuni asupra companiei Visa ca să ia măsuri împotriva instituțiilor financiare care permit această activitate.

La începutul anului 2010, în rețele farmaceutice ilicite și pe siteuri care ofereau antiviruși contrafăcuți s-au infiltrat câțiva cercetători, profesori universitari și studenți la masterat,

care sperau să demonstreze că urmărirea traseului banilor putea contribui la înăsprirea condițiilor pe care aceste afaceri trebuiau să le îndeplinească pentru a beneficia de procesarea cardurilor de credit. Timp de câteva luni, ei au făcut sute de „tranzacții de probă" pe siteurile a 40 de firme dubioase, care vindeau imitații ale unor medicamente care se eliberează pe bază de rețetă, software contrafăcut și produse antivirus false. Cercetătorii – de la George Mason University, International Computer Science Institute și University of California din San Diego (UCSD) – s-au dat drept cumpărători ai acestor produse.

Membrii echipei considerau că, dacă puteau să localizeze instituțiile financiare care profitau de pe urma acestui comerț și să atragă atenția publicului asupra lor, industria în ansamblu va avea de suferit. Motivul era acela că, deși vânzarea pe internet de medicamente contrafăcute, eliberate pe bază de rețetă nu este ilegală în sine, este ilegal ca organizații străine să expedieze în SUA medicamente care nu pot fi procurate decât prin prezentarea unei rețete. O asemenea activitate încalcă regulile de procesare a cardurilor Visa și MasterCard și este pasibilă de amenzi serioase.

După cum am menționat în capitolul 5, profesorul Stefan Savage și echipa sa de la UCSD au depus o muncă enormă doar pentru a strânge date empirice despre industria spamului farmaceutic.

„Când am început treaba asta, spunea Savage, am urmărit să descoperim întregul lanț al afacerilor din economia spamului. O componentă însemnată a acestuia o reprezentau procesarea plăților și băncile, la care nu se uita nimeni."

Savage spunea că, inițial, cei de la University of California din Berkeley nu fuseseră prea interesați de munca lor. Complicatele probleme etice și legale generate de încălcarea, în principiu, a legislației în vederea efectuării unei cercetări de altfel inofensive făceau proiectul greu de acceptat. Universitatea respectivă și cercetătorii au căzut la o înțelegere.

Ei aveau să cumpere doar medicamente generice, disponibile în SUA și fără rețetă, cum ar fi RU-486, pentru întreruperea sarcinii.

S-a dovedit că partea cea mai dificilă a proiectului lor a fost să găsească un mod sigur de a plăti produsele comandate. Dacă ar fi comandat medicamentele cu același card de credit în mod repetat, *partnerka* ar fi anulat tranzacțiile și ar fi trecut numărul cardului pe lista celor dubioase. De aceea, s-a optat pentru carduri-cadou preplătite, întrucât acestea permiteau efectuarea achizițiilor în condiții de anonimat. Nu era totuși suficient să poți cumpăra medicamentele cu carduri preplătite. Echipa de cercetători a trebuit să-i convingă pe emitenții cardurilor să divulge numele băncilor și numerele conturilor comerciale utilizate pentru procesarea tranzacțiilor.

„Am constatat că era cel mai ușor să utilizăm carduri-cadou, a spus Savage, pentru că în ele puteam trece un nume fals. Însă, în cazul multora dintre aceste carduri-cadou, dacă doreai să afli informații despre tranzacții, trebuia să suni la un centru de asistență pentru clienți. Chiar pentru unele dintre cardurile preplătite emise de firme destul de mari, existau doar câteva persoane care acordau asistență clienților. Iar acestea deveneau repede suspicioase pentru că, dacă făceai multe cumpărături, ajungeai să vorbești mereu cu aceiași oameni."

Savage și ceilalți cercetători au descoperit repede rețeaua perfectă, deși el a refuzat să-i dea numele pentru a nu afecta cercetări similare, atât în curs de desfășurare, cât și viitoare. A spus doar că este un card preplătit emis de un lanț destul de mare de supermarketuri din SUA.

„Am întrebat deci un alt grup care analiza această problemă și ne-a spus despre un card-cadou al unui lanț de supermarketuri. Chris Kanich [masterand la UCSD] s-a dus la unul dintre supermarketuri cu vreo 5 000 de dolari și a cumpărat o grămadă de carduri preplătite. Nimeni n-a clipit măcar, a spus Savage. Avem și acum un teanc pe undeva. A fost însă greu să obținem acceptul universității. Urma să luăm toți banii aceia

și să-i transformăm în instrumente de plată care nu puteau fi urmărite. Bineînțeles, trebuia să aibă încredere în noi că nu vom pleca în vacanță în Brazilia sau mai știu eu unde."

Cu acordul universității și cu o grămadă de carduri preplătite de dimensiunea câtorva pachete de cărți de joc, cercetătorii au început să cumpere medicamente contrafăcute de pe siteurile promovate prin spam. Cardurile preplătite au avut mare succes la toate farmaciile on-line și totul părea să meargă ca pe roate. Asta până când unchiul Sam a decis că piața înfloritoare și în mare parte nereglementată a cardurilor preplătite era folosită în mod abuziv de cei care spălau bani.

„Totul a mers bine până când Congresul a hotărât să ajute lumea cu acest Credit CARD Act din 2009, a spus Savage, referindu-se la o lege care a intrat în vigoare în 2010 și includea multiple restricții privind modul în care pot fi taxați consumatorii de către companiile de carduri de credit. Rețeaua de combatere a criminalității financiare (FinCEN) din cadrul Departamentului Trezoreriei a fost întotdeauna foarte preocupată de cardurile-cadou din punctul de vedere al sumelor care nu puteau fi urmărite, fiindcă acestea erau perfecte pentru spălarea banilor. Jur că, dacă aveai o geantă plină cu astfel de carduri, puteai transfera milioane de dolari, iar geanta ar fi fost mult mai ușoară decât câteva milioane de dolari în bancnote."

Industria cardurilor preplătite scăpase cumva de reglementările de tipul „cunoaște-ți clientul", care guvernează toate instituțiile financiare americane. Aceste reglementări impun băncilor să ia anumite măsuri pentru a realiza un profil al activității clienților cu scopul de a găsi indicii privind spălarea banilor, tranzacții suspecte și finanțarea terorismului. După ce Credit CARD Act a fost promulgat, rețelele de carduri preplătite au intrat sub incidența acelorași reguli.

„Toate aceste carduri erau reîncărcabile. Puteai pune pe ele orice nume doreai, pentru că, în esență, nu existau reguli de tipul «cunoaște-ți clientul» pentru cardurile preplătite, a spus Savage. Iar acum, dintr-odată, rețelele care le ofereau aveau

nevoie de protecție împotriva spălării banilor prin tranzacții internaționale. Rezultatul imediat a fost că toți cei din industria respectivă au spus cam așa: «Perfect, deci nu mai există tranzacții internaționale cu carduri preplătite.» În felul acesta, cei 5 000 de dolari ai mei investiți în carduri preplătite s-au transformat instantaneu într-un morman de plastic inutil."

Savage a spus că, în momentul acela, s-a simțit descurajat, fiind gata să renunțe, dar unul dintre masteranzii lui, Chris Kanich, nu s-a dat bătut. Era spre sfârșitul lui noiembrie 2011.

„Afurisitul ăla m-a ignorat complet și a început să ceară oferte de la emitenții de carduri de credit. Le telefona și spunea: «Bună ziua, numele meu este Chris Kanich. Facem o cercetare în domeniul farmaciilor bazate pe spam și avem nevoie de un produs financiar care să poată face asta, asta și asta.» A telefonat la vreo 50 de bănci până a găsit o bancă mică din Midwest. Persoana cu care a vorbit a fost receptivă și i-a spus că directorul lor chiar era interesat de securitatea informatică. Așa că am negociat cu ei o înțelegere specială, după care totul a devenit mult mai ușor."

Echipa de cercetători s-a familiarizat cu diferitele planuri pe care diverse rețele de farmacii ilicite le utilizau pentru a elimina tranzacțiile suspecte. Acestea se fereau de orice fraudă care ar fi putut mări costul tranzacțiilor sau care ar fi putut duce la închiderea lor, așa încât aveau tendința să se bazeze pe mai multe tipuri de măsuri antifraudă. De exemplu, utilizau servicii de localizare pentru a vedea dacă adresa de internet a cumpărătorului arăta că acesta locuia la aceeași adresă cu cea de facturare de pe cardul de credit.

„Cu timpul, am aflat că fiecare tranzacție primea un punctaj de fraudă bazat pe o serie de criterii, iar tranzacțiile care depășeau un anumit punctaj pur și simplu nu erau realizate, spunea Savage. Am aflat că o adresă de e-mail de la un furnizor public de webmail creștea punctajul de fraudă. Am aflat de asemenea că numele trebuia să fie asociat unei

adrese fizice reale și unui număr de telefon valabil, fiindcă, de multe ori, sunau ca să verifice comanda."

Cercetătorii au fost descoperiți destul de repede după ce au început să facă cumpărături. Ei încercau ca, în fiecare lună, să efectueze minimum o achiziție sub acoperire de la fiecare dintre cele peste 20 de programe de parteneriat farmaceutic on-line, astfel încât să poată ține evidența băncilor care procesau tranzacțiile. Nu știau însă că majoritatea parteneriatelor foloseau aceleași instituții financiare: câteva bănci din Azerbaidjan, Letonia, Cipru și Turcia.

„Am încercat să nu ne dăm de gol și să facem o singură comandă pe program în fiecare lună, dar fiindcă nu știam că totul era procesat în același loc, făceam vreo 35 de comenzi pe lună de la aceleași persoane, a spus Savage. La un moment dat, Chris Kanich [care participa în continuare la proiect, dar devenise asistent universitar la University of Illinois din Chicago] a primit un telefon din partea serviciului de asistență pentru clienți al uneia dintre *partnerka* și a trebuit să dea un răspuns rapid, pentru că ei doreau să știe de ce atât de multe persoane de la adresa lui comandaseră Zyrtec, care este un medicament antialergic. Chris a născocit pe loc o poveste, spunând că locuia într-un cămin studențesc și că el și toți colegii lui erau alergici la părul de pisică, iar unul dintre ei avea o pisică. Așa că, în timp, am învățat cu toții cum să facem comenzi false."



## SPAMALYTICS, MICROSOFT ȘI NAPALM

Urmărirea traseului banilor a dezvăluit un fapt surprinzător: 95% din totalul tranzacțiilor cu carduri de credit care au avut ca obiect medicamentele și remediile pe bază de plante promovate prin spam pe care le cumpăraseră cercetătorii erau procesate de numai trei firme financiare: una din Azerbaidjan, una din Danemarca și una din insula Nevis (Indiile de Vest). Probabil că multor americani le-ar fi greu

să găsească aceste locuri pe hartă, cu atât mai puțin să facă afaceri cu firme de acolo. Cu toate acestea, plățile cu card de credit pentru industria spamului erau procesate de instituții financiare din acele regiuni. Experții antispam voiau să știe de ce băncile nu și-au putut da seama de această ciudată concentrare a unor activități bancare dubioase și s-o stopeze.

Cercetătorii au dat publicității concluziile în studiul intitulat „Click Trajectories: End-to-End Analysis of the Spam Value Chain", descriind ceea ce ei numeau „spamalytics", metoda prin care au descoperit slăbiciunea principală a tuturor operațiunilor de spam: dependența de procesarea cardurilor de credit pentru produsele promovate prin mesaje nesolicitate.

Savage a spus că, la cinci zile după ce *New York Times* a publicat un articol despre studiul lor, cercetătorii au fost sunați de la Casa Albă. La telefon era Victoria Espinel, cea care se ocupa de drepturile de proprietate intelectuală în cadrul administrației Obama.

„Avea o întâlnire ultimativă cu reprezentanții administratorilor de nume de domenii, ai unor firme renumite și ai Google, cărora le-a zis: «Ar trebui să facem toți ceva în privința acestei probleme a spamului.» În lucrarea noastră, am spus că, în principiu, existau două moduri de acțiune: se putea acționa împotriva băncilor comerciale [ale farmaciilor] – dar acest proces era lent – sau se putea încerca să se intervină la emitenții cardurilor de credit, deoarece aceste rețele farmaceutice erau finanțate în majoritate din bani occidentali. Privind situația retrospectiv, a fost o idee proastă, pentru că, atunci când am vorbit cu băncile emitente din SUA, acestea ne-au spus: «Clienții noștri nu se plâng și nu e treaba noastră să controlăm ce fac ei atât timp cât, în acte, tranzacțiile par a fi legale.»"

Espinel i-a pus în legătură pe Savage și membrii echipei sale cu International Anti-Counterfeiting Coalition (IACC), o organizație nonprofit creată pentru a ajuta marile corporații să rezolve problema pirateriei comerciale și a folosirii abuzive a mărcilor comerciale. IACC pregătea un portal on-line pe care orice deținător de brand se putea înscrie pentru a raporta direct

MasterCard şi Visa faptul că cineva folosea în mod abuziv brandul său. Cele două firme aveau să analizeze reclamaţia şi, în cele din urmă, să amendeze orice instituţie bancară care procesa tranzacţii legate de reclamaţia respectivă.

IACC funcţionează în baza unor contracte pe care toate băncile le semnează înainte de a face afaceri cu asociaţiile emitente de carduri de credit şi în care se stipulează că vânzările de produse trebuie să fie legale nu numai în jurisdicţia în care se află banca comercială, ci şi în ţara de origine a clientului. Iar pentru că expedierea unor medicamente eliberate numai pe bază de reţetă către clienţi din afara SUA încalcă legile americane, toate reclamaţiile transmise celor de la Visa ori MasterCard prin intermediul IACC de către deţinătorii unor branduri afectate au provocat aplicarea unor amenzi usturătoare băncilor care procesau plăţi pentru *partnerka* farmaceutice.





„Aceste lucruri figurau întotdeauna în contracte, dar, din cine ştie ce motiv, oamenii nu le acordau atenţie, a spus Savage. S-a dovedit că cei cu adevărat interesaţi de problema spamului erau deţinătorii de branduri, întrucât produsele, drepturile de autor şi mărcile lor comerciale erau fie contrafăcute, fie încălcate. Iar frumuseţea acestei abordări este că problema nu ţine de dreptul penal. Ea ţine numai de contracte. De fapt, în acest proces nu e implicată nicio instituţie care veghează la respectarea legii. Este vorba doar de a determina firmele Visa şi MasterCard să vegheze la respectarea prevederilor din propriile contracte."

În mod paradoxal, nu companiile farmaceutice au început să folosească arma IACC împotriva spammerilor farmaceutici, ci Microsoft. Aceleaşi reţele care distribuiau spam pentru promovarea farmaciilor on-line erau utilizate pentru a promova siteuri ce comercializau copii contrafăcute ale sistemului de operare Windows, iar Microsoft a văzut în IACC o şansă excelentă de a mări costurile suportate de falsificatori

în momentul procesării plăților făcute cu card de credit pentru achiziția unor copii piratate de Windows.

„Microsoft a luat decizia să meargă până la capăt. Erau cu adevărat hotărâți, a spus Savage. Ideea lor a fost, așa cum se exprima șeful lor, un fel de «cadou special de Ziua Recunoștinței». Aveau de gând să urmărească simultan toate băncile folosite în acest program, toți administratorii de nume de domenii și toate companiile de hosting, apoi să termine cu toate repede. După aceea, voiau să se ducă la Google și Bing ca să-i prindă și pe spammeri, studiind rezultatele căutărilor. La un moment dat, au aruncat pur și simplu bomba asupra întregii industrii. Iar în subteran are loc o schimbare, căci toată lumea zice: «Hei, avem niște probleme aici.»"

Savage spunea că o mare companie de software a urmărit în mod special programele de afiliere care îi vindeau produsele. Programele de afiliere care comercializează software OEM* piratat se ocupă în special cu vânzarea produselor foarte scumpe, printre care Windows și aplicațiile Adobe. Probabil că, în acest caz, era vorba despre Adobe, având în vedere reacția de pe forumurile de profil.

„Această companie i-a vânat pe toți. A acționat atât de rapid – și nu numai pentru propriile produse – încât aproape că a distrus întregul sistem OEM, spunea Savage. Două [programe de afiliere OEM] au supraviețuit după ce s-au debarasat de brandul acelei companii, dar, la început, când oamenii n-aveau habar ce se întâmplă, n-a mai putut să facă nimeni afaceri."

Contractele dintre bănci, pe de o parte, și Visa și MasterCard, pe de altă parte, stipulează că vânzătorilor li se interzice să comercializeze bunuri și servicii care sunt ilegale în țara în care bunurile sau serviciile respective sunt cumpărate sau utilizate. Asociațiile emitente de carduri de credit au o procedură standard de acceptare a reclamațiilor privind astfel

* „Original equipment manufacturer" – producător de echipamente originale (n. tr.).

de tranzacții, în care avertizează banca vânzătorului on-line (transmițându-i și o notificare cu privire la eventualele amenzi pe care le va primi pentru neconformare). După ce primește o reclamație, banca vânzătorului face propria anchetă și are posibilitatea de a o contesta dacă consideră că plângerea nu este întemeiată. Dacă însă banca decide să nu conteste reclamația, trebuie să ia măsuri pentru a preveni apariția unor situații similare, pentru că, în caz contrar, va primi amenzi din ce în ce mai mari din partea asociațiilor emitente de carduri.

Cercetătorii au observat că, de multe ori, conturile comercianților care fuseseră utilizate în activități frauduloase cu mult timp înainte ca ei să depună o reclamație la IACC nu au mai fost utilizate după mai puțin de o lună de la depunerea reclamației.

Savage a afirmat că, potrivit datelor analizate, sectorul privat poate avea un impact major asupra criminalității informatice prin simpla urmărire a traseului banilor destinați acestor operațiuni.




„Nu este nevoie de un judecător, de un polițist și nici măcar de capacități de securitate sofisticate. Dacă poți să cumperi un produs, atunci acesta este înregistrat undeva, iar înregistrarea respectivă indică contul comercial în care ajung banii, spunea Savage. Cei de la Visa și MasterCard nu privesc cu ochi buni vânzările de produse ilegale făcute pe rețelele lor și vor acționa în consecință în urma reclamațiilor venite de la deținătorii de branduri, bazate pe achiziții sub acoperire."

Cam în aceeași perioadă în care cercetătorii prezentau IACC concluziile lor, Visa adopta o serie de modificări ale regulamentelor sale de funcționare, care păreau a fi îndreptate împotriva farmaciilor on-line și vânzătorilor de mărfuri contrafăcute. În primul rând, vânzările de mărfuri considerate a fi asociate celor farmaceutice au fost catalogate pentru prima dată în mod explicit ca având un „risc ridicat" (alături de jocurile de noroc și diverse tipuri de servicii de marketing direct), iar băncile care încheiau contracte noi cu firme de comerț

electronic cu risc ridicat aveau nevoie de un audit prealabil mult mai complex (inclusiv de un capital propriu de minimum 100 de milioane de dolari și o evaluare bună în cadrul programelor de management al riscurilor).

De asemenea, noile documente conțin în mod explicit exemple de tranzacții ilegale, cum ar fi „vânzarea ilegală de medicamente care necesită rețetă" și „vânzarea de produse sau servicii contrafăcute ori care încalcă proprietatea asupra mărcii comerciale". În sfârșit, aceste modificări includ amenzi mai mari pentru neconformare.

Dovezile cele mai elocvente ale succesului strategiei bazate pe achiziții de probă vin chiar de la cei care se ocupă de programele de afiliere care îi recompensează pe spammeri și pe răufăcători pentru că promovează software piratat și antiviruși falși, precum și de siteurile farmaceutice ilicite. În iunie 2012, șeful unui cunoscut program farmaceutic fraudulos a postat un mesaj lung pe forumul în limba rusă gofuckbiz.com, care se adresează unor asemenea programe de afiliere. În acel fir de discuții, care are în prezent peste 250 de pagini, managerul programului le explică membrilor dezorientați ai forumului motivul pentru care programele farmaceutice au avut atâtea probleme în ceea ce privește procesarea cardurilor de credit.

> În mai 2011, Visa a inițiat un nou program, așa-numitul „Global Brand Protection Program". În momentul acela, nimeni nu știa ce efect va avea asupra băncilor și comercianților, așa că, pentru moment, nu s-au schimbat multe lucruri – totul a continuat să funcționeze ca și înainte. După câteva luni, Visa a început să acționeze și, din noiembrie 2011, asupra comercianților au început să curgă amenzi de câte 25 000 de dolari pentru fiecare domeniu care conținea brandurile Viagra, Cialis și/sau Levitra, sau alte medicamente protejate prin drepturi de autor.

Managerul continua astfel:

Toate programele de afiliere au fost atacate. În prezent, cele mai importante au plătit amenzi de câteva sute de mii în cadrul acestui program. De asemenea, sunt atacate băncile și, deși cele mai multe își pot acoperi pierderile financiare pe seama comercianților – cu condiția să aibă o cifră de afaceri suficient de mare – auditurile efectuate de Visa, riscurile cu privire la reputație și alte chestii le complică activitatea. Acesta este motivul pentru care unele au refuzat să mai facă afaceri, altele au redus considerabil volumul plăților „farma", iar altele s-au „supraasigurat" într-un fel sau altul, ceea ce a dus practic la rate de aprobare zero. Unele (bănci) continuă să lucreze, dar numărul lor este foarte redus în prezent.

Alt afiliat al unui program farmaceutic ilicit a prezentat situația în termeni mult mai puțin delicați, observând următoarele:

> În prezent, majoritatea programelor de afiliere au un număr ridicat de respingeri, refuzuri și amânări, iar după umila mea părere, acest lucru nu ține prea mult de program; imaginea generală este tristă: nenorocita de Visa ne arde cu napalm.

Savage spunea că, după ce au fost pârjoliți de amenzile primite de la Visa, mulți procesatori de tranzacții ale farmaciilor au început să „codifice greșit" dinadins aceste tranzacții. Companiile emitente de carduri de credit solicită ca toate tranzacțiile să aibă un cod care corespunde tipului de produs sau serviciu achiziționat. Există mii de astfel de coduri (de exemplu, domeniul farmaceutic are 5192), iar contractele pe care comercianții trebuie să le semneze cu asociațiile emitente de carduri le dau acestora din urmă puterea de a aplica amenzi uriașe celor care codifică greșit tranzacțiile de risc înalt ca fiind activități cu risc mai scăzut.

„În acest moment, a spus Savage, majoritatea *partnerka* farmaceutice rămase au început să fie disperate și să facă lucruri nebunești, de pildă să-și spele banii trecându-i prin firme care administrează parcări și prin diverse bănci din SUA.

Codificarea greşită era o soluţie excelentă pentru că [iniţial] noi, cercetătorii, nu ne puteam plânge la Visa de majoritatea produselor contrafăcute, fiindcă nu aveam niciun argument faţă de Visa. Nu puteam spune pur şi simplu: «Hei, uitaţi un produs Pfizer contrafăcut. Visa, trebuie să faci ceva în legătură cu asta!» Doar titularul brandului putea să ia măsuri. În privinţa acestor codificări eronate însă, oricine poate raporta orice. Dacă noi descoperim că una dintre aceste farmacii foloseşte o bancă americană şi îşi codifică greşit tranzacţiile, putem adesea să sunăm banca şi să-i spunem: «Hei, ştiaţi că se întâmplă asta?» De cele mai multe ori, banca va spune: «Vă mulţumim foarte mult», deoarece poate primi amenzi mari pentru procesarea tranzacţiilor codificate eronat. Astfel, dacă le spui, ajung să închidă afacerea fără ca Visa să afle şi să le amendeze."

Damon McCoy, lector la departamentul de informatică al George Mason University, spunea că numeroase programe de afiliere care oferă produse farmaceutice, scareware şi software OEM au reacţionat faţă de restricţiile cu privire la plăţi aplicând măsuri de securitate împovărătoare pentru depistarea comenzilor de probă. De exemplu, unele programe farmaceutice ilicite, ca RxPayouts, au început să le ceară cumpărătorilor să trimită prin e-mail sau fax copii după permisele de conducere şi cardurile de credit. Altele au decis să proceseze doar plăţile clienţilor existenţi.

Ambele măsuri de securitate pot fi dăunătoare însă atât pentru clienţi, cât şi pentru afiliaţi. Cercetătorii notează că cerinţa privind fotografierea unui document de identitate impusă de RxPayouts clienţilor noi (adoptată în ianuarie 2012) a provocat rumoaree în rândul afiliaţilor. Potrivit cercetătorilor, un afiliat a scris ca răspuns: „Această regulă nouă mă termină, rata de conversie a noilor clienţi a scăzut [la zero]. Noii clienţi anulează comanda imediat ce află că trebuie să transmită prin fax o legitimaţie cu fotografie la serviciul pentru clienţi."

McCoy spunea că noile cerințe servesc și la protejarea programelor de afiliere de o altă sursă potențială de dureri de cap și de probleme: afiliații dubioși, care se alătură programului doar pentru a încasa comisioanele pentru comenzi plasate cu carduri de credit furate.

„Inițial, programele de afiliere făceau asta pentru a se proteja de hoții de carduri, iar în trecut, dacă exista o cerere de restituire a sumei plătite pentru o achiziție, programul suporta costul operației, spunea McCoy. Acum, dacă sosește o asemenea cerere, ei vor lua banii respectivi din câștigurile ulterioare ale afiliatului."

Cercetătorii au observat că programele de farmacii afiliate au reacționat în ultima vreme și prin înlocuirea medicamentelor de marcă cu echivalentele lor generice (de exemplu, citrat de sildenafil în loc de Viagra, tadalafil în loc de Cialis și așa mai departe). Operatorii acestor programe le spun afiliaților că asemenea măsuri vor elimina problemele legate de branduri și mărcile comerciale și vor diminua astfel capacitatea deținătorilor de branduri de a închide atât siteuri individuale, cât și conturile comerciale asociate.

Rămâne de văzut dacă această ultimă măsură le va permite băncilor care se ocupă cu astfel de afaceri să continue să facă acest lucru fără a fi deranjate de rețelele de carduri de credit, așa cum afirmă managerul citat mai sus, care a postat următoarele aprecieri pe gofuckbiz.com:

„Doar timpul va spune la ce vor duce toate astea. Fie vor înceta toți să mai folosească branduri bine-cunoscute, care sunt foarte bine știute de cumpărători, și vor începe să folosească denumiri indiene generice sau denumirile ingredientelor active, fie vor continua toți să participe la această cursă dementă de genul «care este mai deștept»."

## Capitolul 12

# FINAL DE PARTIDĂ

În iunie 2011, Vrublevski a făcut a doua călătorie neprogramată în Maldive din anul acela. De data aceasta, a fugit din Moscova fiind că fusese anunțat că procurorii pregăteau împotriva lui acuzații penale în legătură cu un atac informatic lansat în iulie 2010 asupra sistemelor companiei Aeroflot de vânzare a biletelor.

Anchetatorii îi arestaseră deja pe frații Igor și Dmitri Artimovici, care se pare că realizaseră și administraseră împreună botnetul Festi. Ambii au negat că ar fi administrat un botnet sau că ar fi expediat spam și au susținut că poliția rusă a pus dovezi în computerele lor. Procurorii ruși obținuseră o mărturisire semnată de Igor, în care acesta afirma că Vrublevski îl angajase ca să atace compania Assist, care procesa plăți pentru Aeroflot. În momentul atacului, ChronoPay se număra printre companiile care licitau pentru obținerea unui contract profitabil de procesare a plăților pentru Aeroflot, iar procurorii susțineau că atacul fusese menit să împiedice Assist să primească din nou contractul. În mod paradoxal, la o lună după atac, Aeroflot n-a acordat contractul niciuneia dintre cele două companii, ci lui Alfa Bank, cea mai mare bancă privată din Rusia.

Autoritățile ruse i-au reamintit lui Pavel că, în Maldive, putea fi arestat și de autoritățile americane sau de alte autorități naționale, așa că s-a întors de bunăvoie la Moscova.

După sosire, Vrublevski a fost arestat și trimis la Lefortovo, o închisoare de înaltă securitate, ca o fortăreață, construită la Moscova în 1881. Aceasta a devenit faimoasă în timpul Războiului Rece, când a fost folosită de KGB pentru izolarea și interogarea deținuților politici. În 1994, Lefortovo a fost preluată de poliția rusă, iar, ulterior, de FSB, succesoarea KGB.

În închisoare, Vrublevski a recunoscut că a comandat atacul asupra lui Assist, dar, mai târziu, a dezmințit acest lucru. Totuși avocatul său, Stanislav Malțev, angajat al ChronoPay, fostul polițist rus care condusese cândva ancheta în dosarul în care Vrublevski fusese acuzat de afaceri ilegale, a susținut că clientul său ar trebui să rămână în libertate până la proces. Instanța i-a respins cererea și a solicitat ca Vrublevski să fie ținut la Lefortovo șase luni înainte de proces, perioada maximă prevăzută de lege pentru acuzațiile care i se aduceau.





„Riscul principal al eliberării lui nu este că el va fugi, ci că le va face ceva rău martorilor, încercând să-i convingă să nu depună mărturie ori să nu ofere informații despre el", a spus Gusev într-o discuție telefonică.

Este o declarație îndrăzneață pentru un bărbat ale cărui jurnale de chat demonstrează că el și Stupin au plătit 1,5 milioane de dolari pentru a se începe urmărirea penală împotriva lui Vrublevski și 50 000 de dolari pentru urmărirea penală a lui Igor și Dmitri Artimovici, frații care – sub pseudonimul comun „Engel" – se spune ar fi folosit botnetul Festi ca să distribuie spam pentru Rx-Promotion și, ocazional, ca să lanseze atacuri distrugătoare împotriva unor siteuri (inclusiv cel împotriva lui Aeroflot pentru care a fost închis Vrublevski).

Următoarele date provin dintr-o conversație pe chat, care se pare că a avut loc între Gusev și Stupin la 26 septembrie 2010. Cei doi deciseseră deja să închidă SpamIt și se gândeau dacă să procedeze la fel cu GlavMed. Vrublevski este numit aici „Paul" (echivalentul occidental al lui „Pavel").

GUSEV: După părerea mea, tu nu-nțelegi pe deplin ce se-ntâmplă de un an încoace. Paul plănuiește fie să mă arunce în închisoare, fie să mă termine. Intențiile lui sunt absolut clare. Există doar două opțiuni: 1 – nu faci nimic și nu plătești nimănui nimic, iar la sfârșit fie mergi la închisoare, fie continui să te ascunzi până la epuizarea tuturor resurselor; 2 – faci exact ce face și el, în același scop.

Gusev îi spune lui Stupin că „orice război costă bani, resurse și celule nervoase. Nu poți merge la război puțin câte puțin – fie lupți până la capăt, fie nu-l începi deloc. Engel ne va face rău tot timpul... Dacă există vreo posibilitate să-l scoatem din joc, ar trebui s-o folosim. 50 000 de dolari înseamnă foarte puțin față de pierderile pe care le-am avut din cauza atacurilor DDoS și față de pierderile pe care le vom mai suferi dacă ne va ataca din nou".

Conversațiile arată de asemenea că, în aceeași perioadă, Gusev a mers la FSB, fiind ademenit să lucreze cu ei și să ofere informații despre marii jucători din industria farmaceutică ilicită.

„Au multe informații și înțeleg foarte bine cum funcționează totul, de unde vin și unde pleacă banii", i-a spus Gusev lui Stupin în ianuarie 2010. FSB, a zis tot el, „are cu siguranță informații despre felul în care circulă banii. În rezumat: dacă vor să mă bage la închisoare, o vor face. Au întrebat și despre tine. Deocamdată, voiau să lucrez pentru ei și să le ofer informații despre alții. Mi-au promis tot felul de avantaje dacă lucrez pentru ei."

Interesant este că discuțiile de pe chat dintre Gusev și Stupin au fost obținute de anchetatorii FSB care-l arestaseră pe Stupin și făcuseră o copie a hard diskului acestuia. Cumva, Engel – poate datorită mitei plătite de Vrublevski – a obținut o copie a acestor conversații și le-a transmis clandestin câtorva surse, inclusiv autorului acestei cărți.

Conversațiile respective au fost prezentate pe larg în cartea de față, dar una dintre cele mai grăitoare și oneste apare

într-un fir de discuții de pe forumul rusesc master-x.com. Acest fir de discuții este plin de comentarii de la spammeri care au fost excluși din afacere ori au pierdut bani din cauza războiului farma dintre Gusev și Vrublevski. În prezent, el cuprinde peste o sută de pagini.

La începutul discuției de pe master-x.com, aproape toți utilizează pseudonime și, în general, încearcă să-și ascundă identitatea reală, dar, cam pe la jumătatea firului, Gusev începe să facă referiri la propria persoană, care îl identifică în mod clar. În această conversație, Gusev devine neobișnuit de irascibil și se lansează într-o serie de tirade din ce în ce mai ostile la adresa lui Artimovici.





Gusev spune că webmasterii ruși au înțeles că războiul farma dintre el și Vrublevski era doar o întrecere, ca să vadă cine are mai mulți bani și mai multe relații. Gusev îl avertizează de asemenea pe Artimovici că Vrublevski ar putea să-și abată furia asupra lui când va ieși din închisoare. (Recunoscând că Vrublevski l-a angajat să execute atacul DDoS asupra lui Assist, Artimovici a pecetluit în esență soarta lui Pavel.)

> Ține minte că Pașa este un om foarte rău. Și are o memorie de elefant! Faptul că m-am descurcat mai bine ca el după ce am părăsit ChronoPay l-a durut foarte mult timp de 7 ani!!! N-a putut să doarmă și a suferit mult! Asta-i invidia. Distruge omul încet, dar sigur. Acum, imaginează-ți în ce stare de spirit se va afla când va ieși de la închisoare. Flămând, furios, abandonat de toți cei care-l lingușeau, fără afaceri și – lucrul cel mai rău – dându-și seama că nu mă va putea băga la închisoare. Cred că psihicul lui nu va putea suporta o asemenea presiune. Și pentru că pe mine nu mă va putea atinge, se va concentra asupra ta și asupra fratelui tău.

Apoi Gusev spune că, de fapt, *el* s-ar putea răzbuna pe Artimovici înaintea lui Vrublevski.

> Însă toate astea sunt gânduri despre un posibil viitor. Revenind la prezent, cred că, oricum, voi ajunge primul la

tine. Te-am avertizat din timp că, dacă încerci să-mi implici familia în conflictul ăsta, consecințele vor fi foarte dure. Te voi găsi personal, îți voi rupe capul și îți voi pune fundul în locul lui – cel mai probabil, nimeni nu va vedea nicio diferență.

Procurorii ruși l-au eliberat pe Vrublevski din închisoarea Lefortovo pe 23 decembrie 2012, cu doar trei zile înainte de ziua lui de naștere. Eliberarea n-a fost nici pe departe un act de milostenie. În conformitate cu legea rusă, șase luni era durata maximă cât putea fi ținut închis cineva în așteptarea procesului.

La câteva ore după întoarcerea sa acasă, Vrublevski posta mesaje pe Twitter și pe blog despre triumfătoarea eliberare. De asemenea, l-a sunat destul de repede pe autorul cărții de față, mai ales pentru a-i povesti despre tratamentul primit și condițiile existente în faimoasa închisoare. Într-o lungă conversație telefonică, Vrublevski a deplâns prezența și discuțiile permanente ale numeroșilor deținuți musulmani care erau închiși cu el la Lefortovo.

„Nu aveam nici măcar apă caldă sau o nenorocită de fereastră, iar becul ardea non-stop, zi și noapte, își amintea Vrublevski. Asta e cea mai strictă închisoare din Rusia și jumătate este plină cu tot felul de teroriști musulmani. Trei luni n-am avut dreptul să comunic cu familia mea... nici apeluri telefonice, nici vizite, nimic. Am auzit doar prostia asta de «Allah, akbar» de cinci ori pe zi!"

Avocatul i-a interzis să discute despre cazul său, dar, ca întotdeauna, el avea o poveste amuzantă de spus despre situația în care se afla. Când un deținut de la Lefortovo urmează să fie eliberat, este informat în mod ceremonios de condamnații mai vechi despre tradiția solemnă de a-și arde ulterior hainele pe care le purta atunci când a ieșit din închisoare. Temându-se că nerespectarea acelei tradiții i-ar putea aduce ghinion, Vrublevski și-a invitat niște prieteni acasă a doua zi după

eliberare pentru a-şi arde hainele pe care le purta când a fost închis şi eliberat de la Lefortovo.

„Imaginează-ţi următoarea scenă, a povestit Pavel, abia stăpânindu-şi râsul. Era o vreme închisă, urâtă, iar noi stăteam în spatele casei cu hainele pe care le-am purtat când am ieşit din închisoare. Fumam în faţa focului şi participam la incinerarea hainelor. Era exact ca-ntr-un film de la Hollywood, nu lipsea decât o muzică dramatică. Vorbeam lucruri serioase, de felul: «Nenică, să nu te-ntorci acolo, bla-bla.» Deodată, nevastă-mea iese în goana mare din casă ţipând: «Pavel, nu pantofii ăia trebuie să-i arzi!» Am ars nişte pantofi Yamamoto scumpi, nu pe ăia cu care venisem acasă de la închisoare!"

În timpul detenţiei, Vrublevski a semnat o declaraţie în care recunoştea că a pus la cale atacul asupra firmei Assist, care procesa plăţile cu carduri de credit pentru compania Aeroflot. Potrivit declaraţiei, el îi ceruse unui angajat al ChronoPay – Maksim Permiakov, specialist în securitatea informaţiilor – să depună 20 000 de dolari în WebMoney într-un portofel electronic deţinut de Igor A. Artimovici, presupusul botmaster al lui Festi şi fost angajat al filialei Sun Microsystems în Rusia. Într-adevăr, un lung fir de e-mailuri din arhiva de mesaje scursă de la ChronoPay conţine informaţii detaliate despre acest schimb.

Arestat de Serviciul Federal de Securitate al Federaţiei Ruse (FSB), Artimovici a semnat o declaraţie similară, afirmând că a fost angajat de ChronoPay să folosească Festi într-un atac împotriva lui Assist. FSB l-a arestat şi pe fratele lui Artimovici, Dmitri, programator liber-profesionist.

Toţi patru – Vrublevski, Permiakov şi fraţii Artimovici – au fost acuzaţi de încălcarea a două articole din Codul penal rusesc: articolul 272, care se referă la „accesul ilegal la informaţii stocate în computer", şi articolul 273, care interzice utilizarea şi distribuirea de malware. Ambele articole prevăd pedepse cu închisoarea de la trei la şapte ani.

Cu toate acestea, în septembrie 2012, instanța de judecată a refuzat să ia în considerare acuzațiile aduse în temeiul celui de-al doilea articol, declarând că dreptul de a-i acționa în instanță pe cei acuzați de utilizarea și distribuirea de malware se prescrisese.

Înainte de începerea procesului, toți acuzații, mai puțin Permiakov, și-au retras declarațiile semnate în închisoare, susținând că, în momentul respectiv, fuseseră supuși de anchetatori unor presiuni psihologice puternice. Artimovici a spus chiar că fusese bătut de polițiști.

Permiakov a recunoscut însă până la urmă rolul jucat și a acceptat să-i ajute pe procurori în anchetă. Pentru mulți care au urmărit procesul îndeaproape, n-a fost o surpriză. Înainte de a se angaja la ChronoPay, Permiakov lucrase în FSB.

Este posibil de asemenea ca Permiakov să fi fost sursa scurgerilor de informații de la ChronoPay. În numeroasele lui declamații și reflecții despre sursa acestor scurgeri, Vrublevski a rămas neclintit în convingerea sa că materialele de la ChronoPay nu fuseseră furate de hackeri, ci fuseseră sustrase de cineva din departamentul IT al companiei. Interesant este că, din arhiva care cuprindea e-mailuri vechi de ani de zile ale aproape tuturor angajaților importanți ai ChronoPay, lipseau în mod vizibil cele ale lui Permiakov.

În tot cazul, procesul lui Vrublevski și al asociaților săi avea fie un exemplu strălucit tocmai al corupției de care fostul director al ChronoPay plănuise de atâta timp să se folosească în avantajul său.

Aeroflot a afirmat că, în urma atacului DDoS, capacitatea sa de a accepta rezervări prin intermediul siteului și al facilităților de procesare a cardurilor de credit a fost invalidată aproape o săptămână și că atacul a costat compania cel puțin 146 de milioane de ruble (aproximativ 5 milioane de dolari). Dar, așa cum remarcau cei de la cotidianul rus *Novaia gazeta*, care au prezentat cazul Vrublevski poate cu mai multă reținere și scepticism decât orice altă organizație mass-media,

judecătoarea speței a făcut referire în decizia sa la daunele financiare, chiar dacă o instanță de arbitraj a refuzat să recunoască cifrele și a respins acțiunea intentată de Aeroflot pentru obținerea unor despăgubiri în urma atacului. Comisia de arbitraj a subliniat că majoritatea clienților care nu putuseră cumpăra bilete de avion on-line și-au făcut pur și simplu rezervare prin intermediul altor servicii ori au cumpărat bilete de la ghișeele Aeroflot.

Spre sfârșitul procesului, în iunie 2013, Vrublevski a fost din nou arestat și închis, sub învinuirea că ar fi încercat să intimideze un martor al acuzării. Procurorii au afirmat că Vrublevski i-ar fi telefonat martorei Nikita Evseeva și i-ar fi oferit bani în schimbul tăcerii. Dar, potrivit ziarului *Novaia gazeta* și altor publicații rusești, semnătura Evseevei, care apărea pe un document în care ea declara că văzuse și confirmase dovezile pe care acuzarea intenționa să le prezinte la proces, fusese falsificată.





Avocații lui Vrublevski au afirmat că Evseeva era de fapt prietena sau iubita ofițerului care investigase atacul DDoS pentru procuratură. Avocații au mai afirmat că Vrublevski o contactase pe Evseeva pentru a o convinge să afirme în instanță că semnătura ei fusese falsificată de anchetatori și pentru a-i oferi banii necesari deplasării la proces.

Avocații lui Vrublevski aveau probabil dreptate când susțineau că semnătura fusese falsificată, este de părere Aleksei Mihailov, expert în securitatea informației, născut la Moscova și stabilit în prezent la New York, care a urmărit cazul cu foarte multă atenție de la bun început și a citit cu aviditate știrile din presa rusească on-line și rarele reportaje apărute în publicațiile occidentale. El explică astfel importanța semnăturii falsificate și a rolului martorului în acest caz:

„În principiu, anchetatorii FSB au falsificat unele dovezi și, din păcate, acest lucru nu este neobișnuit în Rusia. În procesele penale, termenul *panitoi* definește o persoană din exterior – cineva care nu are niciun interes sau nicio legătură cu

cazul, ca în America, unde juraţii sunt persoane alese la întâmplare – care este dusă în camera în care se află dovezile şi trebuie să certifice că totul e în regulă în ceea ce priveşte manevrarea probelor de către procurori. În acest caz, martorul trebuia să verifice că dovezile ridicate de la Artimovici nu au fost compromise. *Panitoi* ar trebui să fie o persoană absolut neutră şi de aceea este foarte ciudat că, în acest caz, era prietena unui anchetator."

Instanţa a ignorat însă dovezile prezentate de apărare şi a confirmat decizia de a-l închide pe Vrublevski pentru tentativa de influenţare a martorilor.

La rândul său, înainte de a fi închis, Igor Artimovici a acordat un interviu pentru *New York Times,* declarând că nu se ocupa de Festi şi că implicarea sa în activitatea ChronoPay se datora unui proiect al acesteia de creare a unui antivirus sub marcă proprie.

Aşa ceva poate să pară ridicol şi neobişnuit pentru o companie care a jucat un rol esenţial în stimularea dezvoltării şi asigurarea prosperităţii industriei antiviruşilor dubioşi – o afacere prin care se urmărea să se stoarcă bani de la victime prin instalarea de malware în computerele acestora, urmată de oferirea spre vânzare a unui produs de securitate inutil, care ar fi eliminat, chipurile, infecţia.

În afirmaţiile lui Artimovici se pare că există totuşi un sâmbure de adevăr. Când l-am vizitat la Moscova în februarie 2011, Vrublevski mi-a povestit despre planurile de lansare a unei soluţii antimalware cu numele de cod ChronoPay Antivirus. Îmi amintesc că amândoi am râs stânjeniţi atunci, dar printre numeroasele documente scurse de la ChronoPay există rapoarte tehnice care fac referire la realizarea unor module de antivirus. Documentele indică faptul că firma angajase programatori care să reproducă versiunea gratuită a programului antimalware Malwarebytes.

La sfârşitul lui iulie 2013, tribunalul a dat verdictul. Toţi cei patru acuzaţi au fost găsiţi vinovaţi. Vrublevski şi fraţii

Artimovici au fost condamnați la câte doi ani și jumătate de detenție într-o colonie penală. Permiakov a primit o pedeapsă mai mică de doi ani, deoarece îi ajutase pe procurori.

Mihailov a spus că, după părerea lui, aproape tot ce i s-a întâmplat lui Vrublevski în legătură cu dosarul său penal – inițierea, ancheta, urmărirea penală, judecata și condamnarea finală – nu avea decât foarte puțin de-a face cu înfăptuirea justiției așa cum o înțeleg occidentalii. Avea însă de-a face cu vechiul său partener de afaceri Gusev și, mai precis, cu mita pe care acesta o dăduse FSB-ului.

Tot după părerea lui, Codul penal și cadrul legal din Rusia nu sunt tocmai adecvate urmăririi în justiție a multor infracțiuni din domeniul înaltei tehnologii.



„Cu mulți ani în urmă, când a apărut prima dată problema hackerilor și a criminalității informatice, guvernul a introdus o lege care stipula că accesul neautorizat într-un computer este ilegal. În cazul acesta, procuratura a susținut că, atacând sistemul informatic al companiei Assist [care procesa plățile cu carduri de credit pentru Aeroflot], hackerii au obținut, în principiu, acces neautorizat la rețeaua Aeroflot pentru că au reușit să blocheze procesarea cardurilor de credit și funcționarea siteului, a spus Mihailov. Nu poți să susții că o astfel de situație este logică sau că are sens din punct de vedere juridic. Procuratura a făcut ceea ce trebuia să facă. De aceea l-au acuzat de treaba asta, deși orice instanță normală ar fi respins acuzația respectivă din capul locului dintr-o mulțime de motive. Procuratura a prezentat într-adevăr unele dovezi care l-au asociat cu frații Artimovici. Se pare însă că fie multe dintre ele au fost falsificate, fie procesul nu s-a desfășurat corect."

Mihailov observa că Aeroflot este deținută în proporție de 51% de statul rus și că atacul asupra unei proprietăți a statului a însemnat o rușine și o bătaie de cap pentru mulți dintre cei care dețineau puterea.

„Se obișnuiește, zicea el, ca firmele să se folosească de elemente corupte din rândul autorităților pentru a se lupta între

ele și a fura clienții celorlalte. Dar când una dintre părți este dispusă să plătească sume mari sau când sunt implicați politicieni, tot procesul se duce pe apa sâmbetei. În asemenea împrejurări, rezultatul este dictat de relațiile politice și de aspectele financiare."

Mihailov a spus că, după părerea lui, Vrublevski a subestimat în foarte mare măsură gravitatea și forța acuzațiilor aduse de inamicii lui.

„Când a ieșit prima dată din închisoare, a încercat să câștige cazul pe fond, ceea ce a fost o mare greșeală și o mare naivitate din partea lui, zicea Mihailov. Poate a simțit că, în culise, avea sprijin financiar, datorită șpăgilor date în trecut autorităților. Din nefericire pentru el, Gusev a găsit în cele din urmă o armă mult mai puternică și s-a impus. Plata a 1,5 milioane de dolari într-o singură tranșă a însemnat un efort serios din partea lui, chiar și după standardele rusești din domeniul corupției. Mă îndoiesc că Vrublevski a cheltuit atât, chiar luând în considerare eforturile lui anterioare de a rezolva problema Fethard și de a-l angaja după aceea pe Malțev ca responsabil cu securitatea. Gusev a câștigat războiul, sau cel puțin bătălia, mărind considerabil potul. Sunt sigur că, acum, Vrublevski ar plăti fără să clipească o sumă de două ori mai mare ca să fie liber, dar, din poziția actuală, îi este mult mai greu să negocieze."

Mihailov a prezis că Vrublevski nu-și va efectua toată condamnarea sau, dacă se va întâmpla totuși așa, faptul că se vorbește foarte mult despre el avea să-i asigure un statut special.

„Pașa este un tip bogat și acel puțin a fost un tip bogat. Locuia în cel mai prosper cartier rezidențial de la marginea Moscovei. Continuă să fie acționar majoritar la ChronoPay. În locul lui, eu aș fi vândut totul ca să scap de închisoare. În Rusia, așa ceva este relativ posibil, dacă nu cumva FSB lucrează împotriva ta. Ei conduc țara. Dacă cineva din FSB a luat 1,5 milioane de dolari de la Gusev, probabil că nu va accepta bani de la Pașa. Există însă un lucru care îl favorizează. Cazul lui a beneficiat de foarte multă atenție, ceea ce înseamnă că Vrublevski

va fi supravegheat în mod special de administrația penitenciarului. S-au publicat sute de articole despre el și despre cazul ăsta. Nu cred că administrația închisorii și guvernul vor ca o figură cunoscută ca el să fie violată sau înjunghiată în închisoare. Mass-media nu i-ar ierta."

Mihailov a adăugat repede că nu este apologetul lui Vrublevski, pe care îl consideră ținta inevitabilă a justiției divine.

„Cel puțin, aceasta a avut un efect pozitiv. Pavel a fost tras la răspundere pentru o foarte mică parte a infracțiunilor pe care le-a săvârșit, a spus el. Procesul a fost evident o farsă, iar procedura n-a fost respectată. Pașa va ieși din închisoare foarte supărat, probabil peste vreun an. Va căuta să se răzbune, și cine știe? Poate că, peste câțiva ani, Gusev va avea aceeași soartă."





Multe dintre previziunile lui Mihailov s-au împlinit. Nu se știe dacă Vrublevski a plătit pentru acest lucru, dar, în iunie 2014 – după ce nu executase nici măcar un an din condamnarea de doi ani și jumătate – a fost eliberat fără nicio explicație publică (din câte am putut să-mi dau seama în urma unor ample cercetări) și i s-a permis să se întoarcă la Moscova, la familia lui.

Presa locală a lăsat a se înțelege că a fost eliberat deoarece guvernul avea nevoie de el. În martie 2014, ca răspuns la sancțiunile aplicate de SUA Rusiei pentru finanțarea și organizarea separatiștilor proruși care provocau tulburări și conflicte armate în Ucraina, Visa și MasterCard au încetat să presteze servicii pentru clienții a cel puțin două bănci rusești imporante. Președintele rus, Vladimir Putin, a reacționat promulgând o lege care prevede crearea unui sistem național de plăți fără numerar din care să nu facă parte companiile emitente de carduri de credit. Aceeași lege impune respectarea, de către furnizorii internaționali de mijloace de plată care operează în Rusia, a unor cerințe noi, foarte stricte.

Într-o discuție telefonică avută la scurt timp după eliberarea sa, Vrublevski mi-a spus că avocații i-au interzis cu

desăvârșire să vorbească despre cazul său. A spus că nu știa de ce fusese eliberat mai devreme, dar nu credea că acest lucru ar fi avut vreo legătură cu sistemul național de plăți.

„Probabil că m-au eliberat fiindcă am fost un pompier bun", a spus el, explicând după aceea că, în ultimele cinci luni de detenție, fusese pompier voluntar în satul care înconjura colonia penală – o fostă zonă minieră din regiunea Reazan, situată la aproximativ 200 km sud-est de Moscova.

„Am văzut lucruri și locuri pe care oamenii n-ar trebui să le vadă, dar am văzut și lucruri amuzante, a spus Vrublevski ca răspuns la întrebările legate de închisoare. De când am ieșit, oamenii mă întreabă despre sistemul național de plăți și eu le răspund: «Frate, glumești? Pot să-ți spun multe despre cum să dai apă la vaci din mașina de pompieri, dar nu știu absolut nimic despre ultimele modificări ale legislației federale!»"

Vrublevski rămâne principalul acționar al ChronoPay, o companie pe care vrea să o vândă cât se poate de repede. Când l-am întrebat dacă își făcea griji că scandalul în care fusese implicat și detenția l-ar putea împiedica să facă asta, mi-a dat de înțeles că ceea ce nu-l omorâse pe el și compania lui îi făcuse mai puternici.

„Tu crezi că BMW este o mașină bună? Compania aia a produs motoare pentru avioanele nemțești în al Doilea Război Mondial. Poftim, ăsta-i răspunsul! Când cineva face un produs bun – și ChronoPay este un produs bun – toate lucrurile astea sunt secundare."

Gusev rămâne în exil, căci în Rusia este urmărit în prezent de autorități sub acuzația de a fi administrat afacerea ilegală a GlavMed și SpamIt. Vrublevski a spus că Gusev se ascunde cu familia în Spania sau Turcia, dar acest lucru n-a putut fi confirmat de altcineva. Indiferent unde ar fi Gusev în prezent, este puțin probabil că va călători prea curând. Într-o discuție din 2011, el a spus că îl îngrijora faptul că Interpolul îl putea da în urmărire generală dacă traversa granițele europene.

„Mă aştept să intru rapid în baza de date a Interpolului, a spus Gusev. Sunt deja în baza de date a poliţiei ruse, aşa că, din păcate, nu pot veni în Rusia. Sunt sigur că Pavel face tot ce poate pentru ca numele meu să ajungă pe lista Interpolului, iar pentru mine ar putea fi foarte periculos să merg cu avionul sau să traversez în alt fel frontierele."

Kimberly Zenz, expertă în criminalitatea informatică la firma Verisign iDefense din Reston, statul Virginia, a urmărit mulţi ani conflictul. După părerea ei, Vrublevski a fost agresorul, fiind doborât de un enorm amor propriu şi un exces de încredere prost înţeleasă.

„Îi place foarte mult să fie în centrul atenţiei, ceea ce infractorilor informatici n-ar trebui să le placă, a spus Zenz. În acest fel însă, se face cunoscut oamenilor în calitate de mare şef şi le dobândeşte respectul pentru rolul jucat în comunitatea subterană."



Potrivit afirmaţiilor lui Zenz, alţii au fost factorii care au acţionat pentru a submina imperiul lui Vrublevski.

„De fapt, el n-a ţinut pasul cu vremea, spunea Zenz. La un moment dat, oamenii s-au plâns că Rusiei nu i-a păsat niciodată de criminalitatea informatică. Şi cred că Pavel a înţeles greşit cât de departe putea merge şi ce anume putea ataca. Acea parte a personalităţii lui care l-a făcut să dezvolte ChronoPay l-a făcut şi să-şi depăşească limitele, să atace Assist şi să creadă că l-ar putea doborî pe Gusev fără să aibă nicio problemă."

Profesorul Stefan Savage de la UCSD a spus că Vrublevski părea obsedat de ideea unei operaţiuni mai ample şi mai originale de piraterie informatică.

„Trebuie să vezi lucrurile în această lumină ca să înţelegi cum a putut avea o companie legală, pe care a implicat-o apoi în afaceri cu medicamente, cu antiviruşi contrafăcuţi şi cu tot felul de chestii, a spus Savage. În mod clar, voia să fie cel mai important. Iar dacă analizezi interacţiunile lui cu alte persoane

de la ChronoPay – şi faptul că apărea mereu la conferinţele Visa despre securitate şi fraudă organizate în Europa – este limpede că se considera un personaj ieşit din comun. Nu trebuia să facă nimic din toate astea pentru a avea un trai bun. Putea să fi rămas în legalitate, deşi este posibil să fi făcut ceea ce a făcut pentru a duce o anumită viaţă. Suspectez de asemenea că încerca să impresioneze un anumit cerc social din lumea criminalităţii informatice."

Cu toate că războiul farma se poate să se fi terminat deocamdată, ameninţarea globală din partea spamului este mai mare ca oricând. Dispariţia multor programe mari bazate pe spam, ca SpamIt şi Rx-Promotion, a coincis cu o schimbare semnificativă, nefavorabilă în privinţa folosirii criminalităţii informatice ca sursă de profit. În primul rând, activitatea desfăşurată de Savage, Microsoft şi deţinătorii de branduri care au colaborat cu International Anti-Counterfeiting Coalition (IACC) pentru a mări costul accesului programelor *partnerka* la procesarea cardurilor de credit a distrus efectiv o mare parte din industria de scareware sau antiviruşi dubioşi pe care ChronoPay o întreţinuse cu atâta grijă. În locul ei a apărut însă o ameninţare mult mai perfidă: ransomwareul.

Similar cu scarewareul, ransomwareul este distribuit cel mai frecvent prin siteuri compromise sau rău-intenţionate care exploatează vulnerabilitatea browserului. În mod obişnuit, în acest caz, escrocii pretind că sunt de la Departamentul Securităţii Interne al SUA sau de la FBI (ori de la autoritatea statală care se ocupă cu anchetele penale din ţara victimei) şi încearcă să-i sperie pe oameni determinându-i să plătească amenzi ca să nu fie urmăriţi penal fiindcă ar fi descărcat, chipurile, imagini cu pornografie infantilă şi conţinut piratat.

Ransomwareul blochează PC-ul victimei până când aceasta plăteşte răscumpărarea sau găseşte o modalitate de a elimina malwareul. Atacurile ransomware criptează toate fişierele de pe PC-ul victimei, „ţinându-le ostatice"

până când victimele plătesc. Acestora li se cere să achite răscumpărarea prin achiziționarea unui card de debit preplătit sau a unui cupon valoric de la magazine din orice colț al lumii. După aceea, trebuie să trimită atacatorilor codul cuponului sau numărul cardului care le permite acestora să încaseze banii.

„Nu cred că ascensiunea ransomwareului este accidentală, deoarece programelor *partnerka* le este mai greu să găsească mereu bănci care să le ajute să proceseze carduri pentru plăți de tip scareware, spunea Savage. Există indivizi care sunt obișnuiți să câștige bani frumoși, pentru care antivirușii contrafăcuți și scarewareul au devenit o problemă, iar farmaciile on-line nu sunt de fapt o opțiune. În sistem există un spațiu liber în care se pot câștiga bani. Nu este deloc întâmplător faptul că aceste operațiuni de ransomware ocolesc în esență planurile tradiționale de plată."



În ultimii ani, am asistat de asemenea la o schimbare vizibilă a felului în care botmasterii folosesc resursele de care dispun. Potrivit firmei ruseşti de antiviruşi şi produse de securitate Kaspersky Lab, în august 2013, procentul de spam din e-mailuri a scăzut la 67%. Pentru a contrabalansa scăderea veniturilor obținute de pe urma e-mailurilor comerciale, tot mai mulți răufăcători își închiriază botneturile pentru a trimite malware, care reprezintă o amenințare mult mai gravă pentru consumatori, în special pentru aceia dintre noi care nu deschid niciodată e-mailurile dubioase ori spamul și nici nu cumpără ceva prin intermediul acestora.

Un exemplu excelent în această privință este botnetul Rustock, care a început să funcționeze în 2007, promovând escrocherii cu acțiuni de tipul *pump-and-dump*. Mult timp, acesta s-a numărat printre principalii promotori ai siteurilor farmaceutice din toată lumea, dar, în ultimii ani, răufăcătorii care-l administrează au folosit resursele acestuia mai mult pentru a expedia malware camuflat în mii de feluri, de la notificări

false din partea unor firme de curierat până la alerte false de audit din partea fiscului. În cele mai multe cazuri, acest malware care fură parole vizează companii mici și mijlocii din SUA și Europa cu scopul de a infecta computerul persoanei responsabile de finanțele firmei. Înarmați cu numele de utilizator și cu parola corespunzătoare contului bancar al companiei, șarlatanii efectuează transferuri din contul victimei în conturile controlate de ei.

Potrivit lui Gary Warner de la University of Alabama din Birmingham, malwareul distribuit prin botnetul de spam Cutwail este una dintre principalele cauze ale preluării frauduloase a controlului asupra conturilor companiilor. Acest flagel este tot mai des întâlnit și afectează anual mii de firme mici, provocând pierderi de sute de mii de dolari companiilor care îi cad victimă.

O altă schimbare notabilă constă în faptul că infractorii informatici care au botneturi proprii încearcă tot mai des să exploateze la maximum fiecare PC infectat, strângând cu grijă toate datele personale (de exemplu, parolele, codurile de licență software și informațiile despre conturile de pe rețele sociale) de la utilizatorii care nu suspectează nimic, iar toate aceste date, spunea Savage, pot fi revândute altor infractori informatici. În plus, acum există mai multe piețe de desfacere ca oricând pentru „produsele" criminalității informatice, astfel încât botmasterii pot scăpa ușor de datele respective. Cu alte cuvinte, este foarte posibil ca, exact în clipa aceasta, un infractor informatic să vă vândă informațiile personale în schimbul unui câștig frumușel.

„Așa cum eschimoșii aveau grijă să folosească absolut fiecare bucățică dintr-o balenă pe care o vânau, asistăm acum la un fenomen asemănător: botmasterii scotocesc cu grijă în computerele infectate și valorifică toate datele pe care le găsesc, spunea Savage. În zilele noastre, deviza pare a fi: «De ce să las pe masă o resursă nefolosită?»"

În timp ce unii folosesc ransomware și recoltarea datelor, Savage spunea că mulți alți foști afiliați și manageri de afaceri

cu scareware, farmacii și software piratat care au eșuat încearcă să descopere următoarea mare senzație.

„Este vremea inovațiilor, iar oamenii caută în mod clar o altă afacere profitabilă, care să fie la fel de bună ca aceea cu farmaciile, care a adus în mod constant mai mulți bani decât orice altă afacere, a spus el. Câteva programe de afiliere încearcă să distribuie cărți electronice și filme piratate, iar altele fac publicitate pentru împrumuturile de scurtă durată. Acum există o mulțime de programe care scriu referate pentru elevi, iar această afacere pare a avea succes deocamdată."

Celălalt factor care influențează industria spamului, spunea Savage, este faptul că mulți afiliați au câștigat mai mult promovând siteuri prin utilizarea așa-numitelor tehnici de „optimizare neagră a motoarelor de căutare", care manipulează rezultatele furnizate de motoarele de căutare. El sublinia că, dintre cele câteva mii de afiliați ai rețelei GlavMed, câștigurile cele mai mari le-a obținut utilizatorul cu pseudonimul „Webplanet", care este un adevărat expert în asemenea tehnici. Acest tânăr și întreprinzător hacker pare să fi câștigat toți banii din păcălirea motoarelor de căutare.

„În prezent, mulți recurg la frauda publicitară sau optimizarea neagră, a spus Savage. Deocamdată, ei își diversifică activitatea și trec printr-un fel de perioadă de regrupare. Iar cei care câștigă bine din spamul farmaceutic fie se restrâng, fie spun: «Da, va trebui să acceptăm profituri mai mici sau să găsim altă nișă.»"

Savage spune că se așteaptă ca industria farmaciilor on-line să dispară în următorii doi-trei ani.

„Vor mai exista câteva mici programe de afiliere, dar mă îndoiesc că vor fi dintre cele mari, ca Rx-Promotion sau GlavMed, spunea Savage. Ele atrag prea multă atenție și presiune din partea sistemelor de carduri ca Visa și MasterCard."

Comentariile lui erau ecoul straniu al cuvintelor rostite de Igor Gusev în timpul ultimei noastre discuții, de la jumătatea anului 2011.

„Este foarte ciudat că unii trebuie să facă atâtea cercetări costisitoare pentru a înțelege că procesarea cardurilor este veriga cea mai slabă a acestei afaceri, spusese Gusev. Ei trebuie să pună presiune pe cei care procesează carduri; aceștia sunt niște monștri care stabilesc reguli stricte numai dacă sunt supuși unei presiuni publice foarte puternice. Cred că deconectarea într-un fel oarecare a comercianților care au legătură cu farmaciile on-line ar fi o lovitură puternică, iar farmaciile on-line ar dispărea în mai puțin de doi ani."

De asemenea, Gusev se întreba cu ce se va ocupa următorul mare *partnerka* după dispariția programelor farmaceutice.

„Cred că următoarea mare afacere va fi legată de domeniul video, audio și poate de rețelele sociale, a spus el. Va fi un fel de serviciu asemănător partajării pe care încearcă s-o ofere acum Google și Apple: să-ți încarci toate fișierele MP3 și video într-un serviciu web astfel încât să le poți accesa de oriunde. Singura întrebare este ce sistem vor folosi pentru facturare și cum vor plăti oamenii."

Gusev a spus că intenționa să facă afaceri în domeniul consultanței și să ajute programele de afiliere on-line să navigheze pe apele agitate, pline de firme dubioase care procesează carduri de credit și de bănci îndoielnice care le susțin.

„Sincer, analizez posibilitatea asta, spunea el. Dintr-un anumit punct de vedere, este o treabă destul de riscantă, pentru că vreau să stau cât mai departe de orice lucru care ar putea duce la alt dosar penal. Din alt punct de vedere însă, pot câștiga niște bani doar oferind consultanță comercianților din această categorie, dacă acceptă să-mi plătească un anumit procent pentru competențele mele, pentru că băncile joacă un rol esențial în acest caz."

Probabil că majoritatea cititorilor acestei cărți n-au comandat niciodată ceva promovat prin e-mailuri nesolicitate sau n-au ingerat medicamente de origine nesigură, care au fost comandate on-line. Există însă o multitudine de feluri în care până și cei mai precauți utilizatori ai internetului ajung

să-i sprijine pe spammeri, escroci și hoții organizați de pe web. Iar acest lucru are aproape întotdeauna aceeași cauză: apatia.

Indiferent de felul cum navigăm pe internet, utilizând un dispozitiv cu sistem de operare Windows, Mac OS X, Linux sau Android, fiecare dintre noi poate juca un rol în combaterea sau încurajarea fraudelor on-line. Ca atare, toți facem parte fie din problemă, fie din soluție. Nu mai există poziționări intermediare. Cei care lansează în prezent amenințări on-line profită de cei care nu își actualizează programele de securitate sau de cei care deschid fără motiv fișierele anexate e-mailurilor nesolicitate și accesează linkuri bizare din e-mailuri, de pe Facebook sau de pe Twitter care par a fi legitime. Pentru mai multe informații despre ceea ce putem face toți pentru a lupta împotriva spamului și a malwareului – și pentru a ne proteja mai bine on-line – vă invit să citiți epilogul acestei cărți.

# EPILOG

## O LUME FĂRĂ SPAM. CUM NE PUTEM PROTEJA DE CRIMINALITATEA INFORMATICĂ



Mulți dintre noi au primit un e-mail cu spam de la un prieten sau de la o persoană iubită, pentru ca, peste câteva minute, să primim un alt mesaj disperat de la aceeași persoană, care ne anunța că i-a fost spart contul de e-mail și ne avertiza să nu deschidem sau să nu răspundem la niciun mesaj trimis de intrus. Fără îndoială că o asemenea situație este alarmantă pentru mulți utilizatori. Mai înspăimântător este însă faptul că, dacă infractorii informatici moderni preiau controlul contului de e-mail (sau al telefonului, tabletei, contului de Twitter sau de Instagram), transformarea acestuia într-un distribuitor de spam este lucrul cel mai inofensiv care ni se poate întâmpla.

De fapt, contul nostru de e-mail nu este important pentru escroci doar pentru capacitatea sa de a distribui spam sau chiar malware și viruși către toate contactele noastre. În funcție de ceea ce facem cu el și de cât timp îl avem, contul nostru ar putea fi mai important decât ne-am imagina.

De exemplu, când ne înscriem la un serviciu on-line, ni se cere aproape întotdeauna o adresă de e-mail. În aproape toate cazurile, persoana care controlează adresa respectivă poate reseta parola oricărui serviciu sau cont asociat – prin simpla solicitare a unui e-mail de resetare a parolei. Contul de

la fondul de pensii, contul bancar sau contul de la societatea de asigurări este legat de contul nostru de e-mail? Un atacator care controlează acest cont de e-mail – fie printr-un atac de tip phishing, fie prin instalarea de malware în PC-ul nostru – poate pur și simplu să viziteze siteurile care gestionează conturile respective, să solicite resetarea parolei, să acceseze un link dintr-un e-mail și să schimbe parolele (și va începe cu parola noastră de e-mail)!

Chiar dacă persoana care preia controlul contului nostru de e-mail nu are timpul sau înclinația de a profita de toate conturile asociate acestuia, ea știe probabil că acele conturi au o valoare de revânzare în lumea subterană a criminalității informatice. Cât costă acele conturi asociate? În subteran, nu există ceea ce se cheamă o bursă a conturilor compromise, dar liste de prețuri postate recent de câțiva neisprăviți care traficheză conturi nefinanciare compromise oferă unele informații în acest sens.





De exemplu, unii băieți răi din subteran vând, pentru doi dolari, nume de utilizatori și parole furate de la conturi active de pe overstock.com, dell.com și walmart.com. Alții vând conturi la fedex.com și ups.com pentru cinci dolari bucata și conturi Apple iTunes începând cu opt dolari. Conturile care vin cu date corespunzătoare adreselor de e-mail asociate cu fiecare site pot fi mai scumpe cu un dolar sau doi.

Unele magazine ale infractorilor au prețuri și mai mici la conturile compromise, cerând doar trei dolari pentru conturi active pe dell.com, overstock.com, walmart.com, tesco.com, bestbuy.com și target.com, pentru a numi doar câteva. Poate părea un mărunțiș pentru care nu merită să te deranjezi, dar nu uitați că băieții răi implicați în această activitate gestionează foarte des botneturi mari, ceea ce înseamnă că pot aduna simultan informații de la sute sau mii de computere compromise.

Chiar dacă adresa noastră de e-mail nu este legată de siteurile unor comercianți on-line, este probabil conectată la alte

conturi pe care le considerăm importante. Conturile de e-mail sparte nu sunt folosite doar pentru a expedia mesaje nesolicitate. Ele sunt căutate şi pentru adresele de e-mail ale contactelor din agenda noastră, care pot fi după aceea bombardate cu malware, spam şi atacuri de tip phishing. Aceleaşi contacte pot primi chiar un mesaj, chipurile, din partea noastră, în care se spune că am rămas fără niciun ban într-o ţară străină şi că le rugăm să ne trimită bani undeva. Credeţi-mă, nenumărate persoane dau curs acestor false rugăminţi de ajutor şi trimit bani direct în buzunarele hoţilor.

Dacă am achiziţionat software, codul de instalare a acestuia se poate să fie stocat undeva în mesajele noastre e-mail. Utilizaţi servicii de stocare a fişierelor on-line sau de tip „cloud" ca Dropbox, Google Drive sau Microsoft SkyDrive pentru a crea copii de rezervă sau pentru a stoca fotografii, fişiere şi muzică? Codul de deblocare a accesului la ele se află de asemenea în căsuţa de e-mail.

Iar cel mai rău este că, dacă contul de webmail a fost spart şi era folosit drept cont de rezervă pentru a primi e-mailuri de resetare a parolei pentru unul dintre celelalte conturi... aţi ghicit, atacatorii pot controla ambele conturi.

Sper că acum este limpede că, pentru a-i împiedica pe hoţi să intre în contul de e-mail, merită să ne luăm măsuri de precauţie. Din fericire, câteva sfaturi simple ne pot ajuta să păstrăm controlul asupra contului de e-mail şi să protejăm PC-ul pe care îl utilizăm pentru accesarea contului respectiv.

Până de curând, unii dintre cei mai importanţi furnizori de servicii on-line ofereau puţine măsuri de securitate în afară de necesitatea introducerii unui nume de utilizator şi a unei parole. Furnizorii mai mari au început să folosească însă autentificarea multifactorială astfel încât utilizatorilor să nu le fie compromise conturile. În prezent, Gmail.com, Hotmail/Live.com şi Yahoo.com oferă posibilitatea autentificării în mai mulţi paşi, pe care utilizatorii pot şi ar trebui s-o folosească

pentru a-şi proteja conturile. Aceasta implică de obicei trimiterea unui cod numeric prin SMS sau printr-o aplicaţie smartphone, care trebuie introdus împreună cu numele de utilizator şi parola. Codul este trimis şi solicitat de fiecare dată când este detectată o conectare suspectă, de exemplu, de la un computer sau o adresă de internet care nu este asociată în mod normal cu contul nostru.

Dropbox, Facebook şi Twitter oferă opţiuni suplimentare de securitate a contului, încurajându-i în acelaşi timp pe utilizatori să aleagă parole puternice. Pentru a verifica dacă adresa de e-mail, reţeaua socială sau alt furnizor de servicii de comunicaţii vă permite să sporiţi securitatea contului prin autentificarea bifactorială, consultaţi siteul twofactorauth.org. Dacă furnizorul are în dreptul numelui său o bifă, daţi clic pe pictograma din coloana „Docs" aferentă numelui său şi se vor afişa instrucţiuni privind configurarea şi activarea acestei funcţii.



## NEBUNIA PAROLELOR

Activarea autentificării bifactoriale este o bună modalitate de a mări securitatea unui cont, dar dacă ne bazăm pe parole slabe, riscul de expunere rămâne mare. În plus, nu toate serviciile sau siteurile importante oferă deocamdată protecţie bifactorială. Aproape nimănui nu-i plac parolele – uneori pot fi greu de ţinut minte – dar, din păcate, nu avem alternativă până la apariţia unor metode mai eficiente de a ne proteja informaţiile de hackeri.* În continuare, vă prezint câteva sfaturi privind crearea unor parole

* Este important să reţineţi că, pentru anumite tehnologii şi dispozitive digitale, se lucrează la metode îmbunătăţite de securitate şi identificare. Multe bănci din Europa, de exemplu, încorporează cipuri în cardurile de credit, ceea ce le face mai greu şi mai costisitor de fraudat. Această metodă este introdusă treptat şi în SUA. O altă măsură de securitate folosită în ultima vreme şi care merită amintită este adăugarea tehnologiei de identificare prin amprentă la unele

puternice. Vă invit să studiați aceste recomandări și instrumente și să vă întăriți acele parole care lasă de dorit.

Dacă semănați cu mine – și detestați realmente parolele, dar recunoașteți că viața este prea scurtă pentru a încerca să țineți minte câteva sute – ar fi bine, poate, să folosiți un manager de parole. Acesta este un software sau un serviciu on-line care îi poate ajuta pe utilizatori nu numai să aleagă și să folosească parole mai puternice, ci și să le protejeze mai bine. Pentru stocarea parolelor, acesta utilizează metode solide de criptare.

Dacă aveți nevoie de ajutor în alegerea unor parole puternice, dar nu sunteți siguri că puteți ține minte unele complicate și lungi ca „#$DG3dcLqziI%&*wp", iată o veste bună: programele de administrare a parolelor sunt concepute să facă exact acest lucru. Aproape toate se conectează la browser, recuperând și inserând parola atunci când vizităm un site pentru care am cerut anterior programului să o țină minte. Tot ce trebuie să facem este să creăm și să ținem minte o singură „parolă principală", puternică, care ni se va cere când vom vizita siteurile respective.

Unele dintre cele mai populare instrumente de administrare a parolelor sunt KeyPass, Password Safe și RoboForm. LastPass este altă opțiune excelentă care funcționează exclusiv on-line. (Nu este nevoie să instalăm pe computer un software special ca să putem accesa parolele indiferent de dispozitivul pe care-l utilizăm – inclusiv smartphone-ul.)

Dacă preferați să vă alegeți și să vă administrați singuri parolele – sau dacă aveți nevoie de o parolă foarte bună pe care s-o utilizați ca parolă principală într-un program de administrare a parolelor – iată câteva sfaturi pentru evitarea parolelor slabe:

- Creați parole unice dintr-o combinație de cuvinte, numere, simboluri, folosind atât litere mari, cât și litere mici.

telefoane și laptopuri, ca opțiune pentru a le bloca sau a le debloca. Fără îndoială, vor urma și alte măsuri.

• Nu folosiți ca parolă numele de utilizator al rețelei.

• Nu folosiți parole ușor de ghicit, cum ar fi „parola" sau „utilizator".

• Nu alegeți parole bazate pe informații care pot să nu fie atât de confidențiale cum v-ați aștepta, ca ziua de naștere, CNP-ul, numărul de telefon, numele membrilor familiei sau ale animalelor de companie, sau orice alt lucru despre care vorbiți pe rețelele sociale. (Băieții răi folosesc și ei Facebook, Twitter și Instagram!)

• Nu folosiți cuvinte care se pot găsi în dicționar. Instrumentele de spargere a parolelor, disponibile gratuit on-line, conțin de cele mai multe ori dicționare cu mii de parole și denumiri comune. Dacă trebuie să folosiți cuvinte din dicționar, încercați să adăugați o cifră și semne de punctuație la începutul sau la sfârșitul cuvântului (ori în ambele poziții).

• Evitați să folosiți combinațiile simple de taste adiacente pe tastatură. De exemplu, „qwerty", „asdzxc" și „123456" sunt parole slabe și foarte ușor de spart.

• Unele dintre parolele cel mai ușor de reținut nu sunt cuvinte în sine, ci serii de cuvinte care formează o frază sau propoziție, poate prima propoziție a unui roman preferat sau prima propoziție a unei glume bune. Complexitatea este desigur importantă, dar lungimea este esențială. Alegerea unei parole alfanumerice lungi de opt până la zece caractere a fost mult timp o practică destul de eficientă. În prezent însă, hackerii și spammerii creează instrumente foarte puternice și rapide de spargere a parolelor, care pot realiza zeci de milioane de combinații de parole posibile pe secundă. Țineți minte că fiecare caracter alfanumeric pe care-l adăugați unei parole sporește înmiit dificultatea atacării ei prin metode brutale ca aceasta.

• Evitați să folosiți aceeași parolă pe mai multe siteuri. În general, puteți utiliza fără probleme aceeași parolă pe siteurile care nu stochează informații importante despre dumneavoastră (siteuri de știri sau forumuri de discuții), cu condiția să nu utilizați aceeași parolă pe siteurile importante.

• Nu folosiți niciodată parola contului de e-mail pe alt site. Dacă faceți asta și un site de comerț electronic la care sunteți înregistrat este spart, există riscul ca e-mailurile dumneavoastră să fie citite în curând de altcineva.

• Indiferent ce faceți, nu păstrați lista de parole pe computer. Este ca și cum ați preda identitatea dumneavoastră infractorilor informatici dacă vă este spart computerul. De-a lungul timpului, opiniile mele cu privire la oportunitatea păstrării unei liste scrise de parole au evoluat. Tind să fiu de acord cu expertul în securitate Bruce Schneier, care îi sfătuiește pe utilizatori să nu-și facă griji că, dacă își vor scrie parolele, cineva le va descoperi. Asigurați-vă doar că informațiile nu sunt păstrate la loc vizibil. Cea mai sigură metodă de a ține minte parolele este să creați o listă cu toate siteurile pentru care aveți parole și, lângă fiecare, să scrieți numele cu care vă conectați și un indiciu care să aibă sens doar pentru dumneavoastră. Dacă vă uitați parola, majoritatea siteurilor vă vor trimite un e-mail cu aceasta (presupunând că vă amintiți cu care dintre adresele de e-mail v-ați înscris).



## FACEȚI ACTUALIZĂRI

Niciun instrument de securitate nu va împiedica accesul altcuiva la căsuța de e-mail sau la contul de Facebook în cazul în care computerul dumneavoastră este compromis de malware care fură parole. Desigur, instalarea pe calculator a unui software antivirus și a unui firewall poate contribui la prevenirea amenințărilor, totuși ele nu sunt nici pe departe o soluție universal valabilă, iar amenințările informatice din prezent sunt făcute în așa fel încât să nu fie detectate de acestea, mai ales în perioada critică a primelor 12–24 de ore în care malwareul este distribuit prin intermediul spamului și al linkurilor de pe siteurile de socializare.

Este important de înțeles că un principiu-cheie în securizarea oricărui computer este cel de „apărare în adâncime", adică crearea mai multor niveluri de securitate pentru a nu depinde prea mult de o singură abordare sau tehnologie în blocarea tuturor atacurilor. Știți însă care este cel mai important nivel dintre toate? Chiar dumneavoastră!

Memorați și aplicați cele trei reguli ale lui Krebs pentru siguranța on-line și veți reduce drastic șansele de a vă lăsa computerul sau dispozitivul mobil la dispoziția celor răi. Pe scurt, acestea sunt:



• Regula 1: *Dacă nu l-ai căutat în mod expres, nu-l instala.* Foarte multe amenințări on-line se bazează pe convingerea utilizatorului de a întreprinde anumite acțiuni – indiferent dacă este vorba despre accesarea unui link, deschiderea unui fișier anexat unui e-mail sau instalarea unei extensii personalizate a browserului ori a unei aplicații. De regulă, aceste atacuri se manifestă sub forma unor mesaje care apar brusc, încercând să-i determine pe utilizatori să instaleze un program de diagnosticare a vulnerabilității computerului. Alte mesaje vă direcționează către un videoclip, menționând că trebuie să instalați un „codec" special, un player video sau o aplicație pentru a-i vizualiza conținutul. Instalați software, actualizări de software sau extensii pentru browser doar dacă le-ați căutat în mod expres. Înainte de a instala ceva, este bine să descărcați programul *direct de la sursă*. Siteuri ca MajorGeeks.com și Download.com susțin că examinează cu atenție programele pe care le oferă pentru descărcare. Însă, așa cum n-ați cumpăra un produs on-line fără a vă fi interesat în prealabil despre calitatea și performanțele sale – și fără să vă fi asigurat că este într-adevăr ceea ce vă doriți – este indicat să pierdeți câteva minute căutând și citind comentariile și recenziile altor utilizatori despre programul respectiv, pentru a vă asigura că nu primiți mai mult decât vă doriți. De asemenea,

evitați să răspundeți în mod direct la alertele prin e-mail care par să vină de la Facebook, LinkedIn, Twitter, de la banca dumneavoastră sau de la alte siteuri care dețin informații despre dumneavoastră. Accesați acele siteuri utilizând un bookmark și gestionați-vă astfel rețelele sociale. Scrierea greșită a unui singur caracter dintr-o adresă de web vă poate duce pe siteuri ostile, făcute să profite de greșelile de scriere.

• Regula 2: *Dacă l-ai instalat, actualizează-l!* Ținerea la zi a sistemului de operare cu ajutorul celor mai recente patchuri (de exemplu, de la Microsoft, Apple sau Google) este importantă, dar pentru a avea un computer sigur, trebuie să aveți grijă și de aplicațiile care rulează peste sistemul de operare. Băieții răi atacă în mod constant vulnerabilitățile unor programe folosite pe scară largă, ca Java, Adobe PDF Reader, Flash și QuickTime. Producătorii acestora furnizează de mai multe ori pe an actualizări pentru a repara erori de securitate, deci este important să aveți ultima versiune a acestor produse. Unele dintre ele îi pot avertiza pe utilizatori că există actualizări, însă anunțurile respective sosesc adesea după mai multe zile sau săptămâni de la lansarea patchurilor. O resursă excelentă pentru oricine este plictisit să caute actualizări o constituie Personal Software Inspector de la Secunia, un instrument gratuit care scanează periodic și îi alertează pe utilizatori în privința programelor de securitate neactualizate. Versiunea cea mai recentă poate fi de asemenea configurată să actualizeze automat aceste produse. Pe FileHippo există de asemenea un bun program gratuit care verifică existența unor actualizări.

• Regula 3: *Dacă nu mai ai nevoie de el, dezinstalează-l!* Dezordinea este dușmanul computerelor rapide. Din nefericire, mulți producători de PC-uri prevăd sistemele pe care le vând cu foarte multe aplicații preinstalate, pe care majoritatea clienților nu le utilizează niciodată. Pe lângă aceste programe inutile, provenite direct de la producător, un utilizator

mediu tinde să instaleze de-a lungul anilor zeci de programe și add-onuri. Pe ansamblu, acestea pot afecta performanța computerului. Multe programe se adaugă singure pe lista celor care se încarcă automat la fiecare pornire a PC-ului, ceea ce face ca pornirea să dureze din ce în ce mai mult. În plus, nu uitați: cu cât ați instalat mai multe programe, cu atât va trebui să dedicați mai mult timp actualizării lor cu cele mai recente patchuri de securitate.

Sper că veți găsi aceste sfaturi utile și oportune. Pentru mai multe informații despre cum să fiți în siguranță on-line – inclusiv pentru informații despre cele mai recente amenințări, planuri infracționale și erori de software care sunt exploatate de spammeri și escroci on-line, vizitați siteul meu, denumit KrebsOnSecurity.com. Dacă veți ajunge acolo, spuneți-mi părerea dumneavoastră despre această carte, utilizând formularul de contact de la www.KrebsOnSecurity.com/about.

# MULȚUMIRI

Scriitorii tind să fie indivizi solitari, însă rareori produc opere plăcute de lungimea și complexitatea unei cărți fără foarte mult ajutor și multă răbdare din partea prietenilor și colegilor.

*Națiunea Spam* nu s-ar fi născut fără ajutorul mai multor vorbitori nativi de rusă, care au petrecut nenumărate ore cu mine, descâlcind conversațiile și legăturile dintre diversele personaje reale care au fost prezentate în carte. În special, aș dori să le mulțumesc lui Alek Geldenberg, Aleksei Mihailov și Maxim Suhanov pentru efortul neobosit depus în traducerea documentelor, e-mailurilor și conversațiilor de chat și, în general, pentru că m-au ajutat să înțeleg diverse aspecte.

Pentru cunoștințele lor despre lumea subterană a hackerilor, recunoștința mea sinceră se îndreaptă către Lawrence Baldwin, Adam Drake, Alex Holden, Lance James, Jon O și Kimberly Zens.

Pentru că m-au ajutat să structurez și să interpretez un volum copleșitor de date, le sunt deosebit de recunoscător lui Damon McCoy, Stefan Savage, Brett Stone-Gross, Gary Warner (și armatelor lor de masteranzi).

Joe Menn și Misha Glenny m-au încurajat și mi-au dat sfaturi înțelepte exact când aveam nevoie. Dacă n-ar fi fost discuția lungă de câteva ore purtată cu Roland Dobbins la Snowmageddon 2009, s-ar putea să nu fi avut curajul să

pornesc pe cont propriu ca jurnalist independent. Mulțumirile mele se îndreaptă și spre J.B. Snyder, un om minunat, care face mereu ceea ce își propune.

Siguranța mea fizică și on-line se datorează, într-o măsură mai mare decât vreau să recunosc, multor persoane. Chris Barton ne-a ferit, pe mine și siteul meu, de atacuri adesea nimicitoare. Group-IB și Kaspersky Lab au avut un rol esențial în a-mi asigura protecția la Moscova. Diverși reprezentanți anonimi ai autorităților mi-au fost de ajutor aici, în SUA; le mulțumesc tuturor.

Nu în ultimul rând, aș dori să le mulțumesc cititorilor fideli ai siteului meu – KrebsOnSecurity.com – pentru încurajarea, sprijinul și inspirația din ultimii cinci ani. N-aș fi putut face asta fără voi.

# SURSE

CAPITOLUL 1 – PARAZIT

Postarea de pe blogul ThreatExpert din noiembrie 2008 (în prezent deținut de Symantec) m-a ajutat să aflu informații despre cursa care a dus la moartea lui Kolea McColo, la fel și un reportaj despre accident apărut în publicația rusă *Rossiiskaia gazeta* (rg.ru). De asemenea, m-am bazat pe mesaje de pe forumul Crutop.nu, precum și pe conversațiile dintre Stupin și Igor Gusev despre cine avea să participe sau cine a participat la înmormântarea lui McColo. În privința informațiilor despre Dmitri „Gugle" Necivolod, m-am bazat pe conversațiile avute pe mesageria instantanee cu Igor Vișnevski.

CAPITOLUL 2 – BULLETPROOF

Multe dintre informațiile generale despre RBN sunt de la surse din Rusia și Belarus, printre care compromat.ru și Transitions Online, precum și din documentarul lui Victor Ceamkovski, *Operation Consortium*, al cărui text este încă disponibil on-line la web.archive.org/web/20120112081516/http:/www.detektiv.by/komputer. Legătura dintre Aleksandr Rubațki și RBN a avut de asemenea la bază o scrisoare adresată guvernului rus de către parlamentarul Ilia Ponomarev. Paragraful referitor la răpirea lui Petrovski s-a bazat pe surse din presă și reportaje, inclusiv *Ecommerce Journal* (web.archive.org/web/20120611001710/http://m.ecommerce-journal.com/articles/hild_adult_in_internet_what_are_the_roots) și ziarul electronic belarus *Diary*. Paragraful despre rolul jucat de furnizorul rus de comunicații Eltel în RBN a avut la bază un articol publicat în 2009 în *Russian*

*Newsweek*. Eltel pare să fi fost achiziționat între timp de Beeline, una dintre cele mai mari companii de telefonie mobilă din Rusia.

CAPITOLUL 3 – RĂZBOIUL FARMA

Datele care susțin declarațiile despre legătura aparentă dintre Vrublevski și Red & Partners au fost publicate pentru prima oară la 31 iulie 2009 în *Washington Post*, în articolul intitulat „Following the Money: Rogue-Antivirus Software" (voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html). Am reluat acest subiect într-o postare din mai 2010 pe KrebsOnSecurity.com, intitulată „Following the Money, Part II" (krebsonsecurity.com/2010/05/following-the-money-part-ii/).

Documentele publice obținute de la Camera de Comerț din Olanda, care se referă la Red & Partners și care arată că Igor Gusev (DPNet) și Pavel Vrublevski (Red & Partners) au creat ChronoPay în 2003 și au devenit acționari cu părți egale, pot fi vizualizate on-line la: krebsonsecurity.com/wp-content/uploads/2011/02/CP20051.pdf. (Notă: acesta este un document olandez dat publicității.)





Sunt greu de precizat cu exactitate sursele unora dintre informațiile care stau la baza acestui capitol. De exemplu, deși se presupune că Gusev sau hackerii apropiați lui au obținut și au făcut publice e-mailuri, documente și înregistrări telefonice de la ChronoPay care acoperă o perioadă de câțiva ani, nu am reușit să confirm acest lucru. După cum se precizează în acest capitol, informațiile au fost transmise de o sursă care a folosit pseudonimul „Boris". În același timp însă, Vrublevski, director al ChronoPay, a confirmat că documentele respective au fost furate, de fapt, de la ChronoPay. Datele despre GlavMed și SpamIt – care cuprind conversații desfășurate pe chatul ICQ timp de patru ani între Dmitri Stupin, administratorul GlavMed–SpamIt, și colaboratorii și angajații săi (spammeri) – au fost cumpărate și transmise autorului acestei cărți și autorităților americane de către Vrublevski.

CAPITOLUL 4 – SĂ-I CUNOAȘTEM PE CUMPĂRĂTORI

Acest capitol s-a bazat aproape în totalitate pe discuții cu persoane care au cumpărat medicamente de la GlavMed–SpamIt și Rx-Promotion. De asemenea, am inclus citate și păreri din conversații on-line

cu Igor Vișnevski, care se declară spammer și care a recunoscut că a finanțat și a revândut botnetul de spam Cutwail. De asemenea, m-am bazat pe informații din surse guvernamentale, inclusiv FDA (www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm229010.htm).

CAPITOLUL 5 – RULETA RUSEASCĂ

În povestea morții Marciei Bergeron, m-am bazat pe un articol apărut în 2007 în *Vancouver Sun*. Pentru informații suplimentare despre acest subiect, am obținut o copie a raportului autopsiei lui Bergeron de la autoritățile din Columbia Britanică.

În acest capitol mă refer la sau citez pe alocuri din articole apărute în *New York Times*. În paragraful cu privire la faptul că medicamentul antiacneic Accutane a fost supus unor noi norme de siguranță de către Food and Drug Administration (FDA) am folosit informații dintr-un articol scris de Gardiner Harris și publicat în august 2005. Un articol semnat de Harris și Katie Thomas, apărut în aprilie 2013 în *New York Times*, m-a ajutat în studiul rolului firmelor indiene care produc medicamentul antileucemic Gleevec la prețuri considerabil mai scăzute decât companiile farmaceutice occidentale.

Un reportaj CNN realizat de David Goldman a fost sursa informațiilor despre amenda de 500 de milioane de dolari pe care Google a plătit-o Departamentului de Justiție din SUA pentru ca acesta să-și retragă acuzația că firma a permis ilegal unor farmacii canadiene on-line să promoveze medicamente către consumatorii americani. O discuție despre suma de 2,3 miliarde de dolari pe care Pfizer a acceptat s-o plătească Departamentului de Justiție a avut la bază informații dintr-un articol semnat de Ron Winslow și apărut în *Wall Street Journal*.

Acest capitol se referă la un incident care fusese prezentat în presă pe când eram în vizită la University of Alabama din Birmingham (UAB) – cazul așa-numitului „canibal de sub pasarelă", despre care s-a spus că a mâncat fața unui om fără adăpost după ce ar fi ingerat săruri de baie. În acel moment, laboratorul UAB testa compoziția chimică a unei substanțe bănuite de autorități a fi săruri de baie. Dar, așa cum au anunțat ulterior CNN și alte posturi de știri, în urma testelor toxicologice efectuate asupra suspectului împușcat de poliție, nu s-au găsit săruri de baie, ci marijuana.

Acest capitol face referire și la un studiu realizat de Merck. Studiul respectiv n-a fost publicat oficial niciodată; referirile sunt, de fapt, la informații on-line pe care Merck le-a strâns între 2009 și 2010 și le-a transmis la cererea autorului.

Paragraful în care se amintește despre o scrisoare a FDA către presupusul partener al lui Vrublevski de la Rx-Promotion se referă la scrisoarea datată 8 octombrie 2010 și adresată lui „Jorge Smark" la adresa de e-mail hellmanh@gmail.com. A se vedea www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm229010.htm.

CAPITOLUL 6 – PARTENER ÎN CRIMA (DEZ)ORGANIZATĂ

M-am inspirat pentru acest capitol în special din studiul fundamental dedicat programelor *partnerka* intitulat „The Partnerka – What Is It, and Why Should You Care", de Dmitry Samosseiko, de la SophosLabs Canada. Acest capitol se bazează de asemenea, în mare măsură, pe datele strânse de cercetătorii de la University of California din San Diego, International Computer Science Institute și George Mason University.



CAPITOLUL 7 – SĂ-I CUNOAȘTEM PE SPAMMERI

Un paragraf în care se vorbește pe larg despre ascensiunea autointitulatului spammer Igor Vișnevski face trimitere la articolul „The Sleazy Life and Nasty Death of Russia's Spam King", de Brett Forrest, publicat în august 2006 în revista *Wired*, în care era intervievat și Vișnevski însuși. Unele informații despre botnetul lui Vișnevski – Cutwail sau „0bulk Psyche Evolution" – provin dintr-un studiu din martie 2011, prezentat la al patrulea simpozion USENIX de către cercetătorii în domeniul securității informatice Brett Stone-Gross, Thorsten Holz, Gianluca Stringhini și Giovanni Vigna și intitulat „The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns".

Unele informații despre legătura existentă între faimosul spammer Piotr Severa și spammerul condamnat Alan Ralsky provin dintr-un rechizitoriu de patruzeci de pagini pe care Departamentul de Justiție l-a depus împotriva lui Ralsky. Date primare despre capacitatea celor mai importante botneturi de a distribui spam provin în special din rapoarte publicate de Dell SecureWorks și M86 Security.

CAPITOLUL 8 – PRIETENI VECHI, DUȘMANI ÎNVERȘUNAȚI

O discuție despre raidurile efectuate asupra companiilor rusești face trimitere la un studiu prezentat la 20 aprilie 2009 de Brenden Carbonell, Dimitry Foux, Vera Krimnus, Ed Ma și Lisa Safyan, din promoția 2010 a Wharton School's Lauder Institute, University of Pennsylvania, și intitulat „Hostile Takeovers: Russian Style" (a se vedea knowledge.wharton.upenn.edu/article/hostile-takeovers-russian-style/). Parte despre Skolkovo, parcul tehnologic de la marginea Moscovei, pe care conducătorii ruși și-l închipuiau ca pe un Silicon Valley al Estului, a avut la bază un articol din martie 2012 al lui Ingrid Lunden de la TechCrunch. Pentru acest capitol m-am inspirat de asemenea din articolul „E-Mail Spam Falls after Russian Crackdown", publicat în octombrie 2010 în *New York Times*.

CAPITOLUL 9 – ÎNTÂLNIRE LA MOSCOVA

Un paragraf care explică motivul probabil pentru care poliția rusă a întreprins un raid la petrecerea organizată de Rx-Promotion face aluzie la o serie de raiduri realizate de poliție în localurile moscovite de jocuri de noroc, despre care au publicat, în februarie 2011, articole pline de culoare Svobodanews, RIA Novosti și *Rossiiskaia gazeta* (rg.ru).

La începutul discuției mele cu Vrublevski, acesta face o referire indirectă la Said Amirov, de patru ori primar al capitalei Daghestanului. Pentru detalii despre arestarea lui Amirov și procesul intentat acestuia pentru un presupus trafic de arme, m-am bazat pe reportaje din *Moscow Times* și de la Business FM Radio.

CAPITOLUL 10 – ANTIS

Informațiile despre procentul e-mailurilor care conțineau reclame nesolicitate din a doua jumătate a anului 2013 provin din statisticile publicate de Kaspersky Lab într-o postare din noiembrie 2013 de pe blogul propriu, securelist.com. Povestea despre atacul asupra lui Blue Security se bazează pe articolul meu despre acest incident, publicat în *Washington Post*. Paragraful despre atacurile din martie 2013 asupra lui Spamhaus are la bază articolele despre Sven Olaf Kamphuis, publicate în martie și aprilie în *New York Times*.

CAPITOLUL 11 – ÎNCHIDERILE

Un articol publicat în martie 2013 în *Milwaukee Journal Sentinel* a fost sursa informațiilor despre recunoașterea vinovăției de către spammerul condamnat Oleg Nikolaenko. Alte referiri la închideri de botneturi și spammeri din acest capitol se bazează pe reportajele scrise de mine despre aceste evenimente și publicate pe KrebsOnSecurity.com.

CAPITOLUL 12 – FINAL DE PARTIDĂ

Începutul acestui capitol include informații dintr-un articol despre Igor A. Artimovici, intitulat „Online Attack Leads to Peek into Spam Den" și apărut în septembrie 2013 în *New York Times*. Ziarele rusești *Vedomosti, Novaia gazeta* și agenția de presă RIA Novosti au fost indispensabile în obținerea de informații despre procesul complicat al lui Vrublevski.

Potrivit mai multor ziare și agenții de presă rusești, Maksim Permiakov a fost singurul dintre cei patru acuzați din procesul lui Vrublevski care a recunoscut rolul jucat în planul de angajare a fraților Artimovici de către Vrublevski în vederea lansării unui atac DDoS împotriva companiei Assist (care concura direct cu firma lui Vrublevski pentru un contract profitabil de procesare a cardurilor de credit pentru cea mai mare companie aeriană din Rusia).

# GLOSAR

**Add-on** – program accesoriu al unei aplicații software menit să-i dea acesteia un plus de funcționalitate.

**Atac DDoS *(distributed denial of service)*** – încercare de blocare a accesului la un serviciu on-line prin supraîncărcarea traficului cu pachete de date din mai multe surse.

**Black hat hacker** – hacker rău intenționat.

**Bookmark** – funcție a unui browser de internet care permite salvarea unei adrese în vederea accesării ei ulterioare.

**Botmaster** – manager de botnet.

**Botnet** – grupuri de calculatoare piratate, în care a fost instalat software perturbator („malware"), menit să le permită atacatorilor să controleze de la distanță sistemele respective fără ca proprietarii lor să-și dea seama de acest lucru.

**Codec** – dispozitiv sau program de codificare sau decodificare a unui semnal digital sau a unui flux de date digitale.

**Farmacii on-line canadiene** – această expresie nu se referă la farmacii situate efectiv în Canada, ci la farmacii on-line care le oferă cumpărătorilor, în special din Statele Unite ale Americii, medicamente mai ieftine, pentru care, de regulă, în SUA, se solicită rețetă.

**Farmacii on-line ilicite** – farmacii care își desfășoară activitatea parțial sau exclusiv pe internet și care livrează prin poștă produsele comandate de clienți. Farmaciile on-line ilicite sunt principalul canal comercial folosit în Occident pentru vânzarea produselor medicale falsificate. Siteurile lor pot fi accesate

cu ușurință, prin intermediul e-mailurilor nesolicitate sau al motoarelor de căutare.

**Găzduire bulletproof *(bulletproof hosting)*** – serviciu pus la dispoziție de unele firme de găzduire web sau de domenii care manifestă o toleranță maximă în ceea ce privește materialele pe care clienții le pot încărca sau distribui. De această toleranță profită spammerii, agențiile de pariuri on-line și cei care oferă pornografie ilegală.

**Malware** – program sau fișier destinat să producă pagube sistemului informatic în care este executat. Din categoria programelor malware fac parte virușii, viermii, troienii, programele ransomware și spyware. Ele pot îndeplini diverse funcții, ca de exemplu: furtul, criptarea sau ștergerea unor date importante, modificarea sau preluarea controlului asupra unor funcții de bază ale sistemului informatic, urmărirea activității desfășurate la calculator fără permisiunea utilizatorului acestuia.



**Money mule** – persoană care transferă bani obținuți prin mijloace ilegale între diferite conturi bancare, în numele unor terți.

**Patch** – mic program informatic care poate fi adăugat unui program existent pentru a-l face să funcționeze normal.

**Peer-to-peer** – arhitectură de rețea pentru aplicațiile distribuite, care împarte sarcinile la mai mulți parteneri, permițând computerelor să se conecteze în mod direct între ele, pentru partajare de fișiere.

**Phishing** – activitate infracțională prin care se urmărește obținerea, de regulă de la clienții unei organizații, prin intermediul unui e-mail, a unor date personale sau confidențiale.

**Ransomware** – program din categoria malware menit să infecteze un sistem informatic și să cripteze datele existente în acesta. După ce programul a fost instalat în sistemul-gazdă, infractorii solicită victimei plata unei răscumpărări în schimbul decriptării datelor.

**Scareware** – program menit să-l determine pe utilizator să cumpere și să descarce software inutil și potențial periculos, cum ar fi antiviruși falși.

**Spammer** – persoană care trimite, unui număr mare de destinatari, mesaje e-mail nesolicitate, de cele mai multe ori cu caracter publicitar.

**Spyware** – program din categoria malware cu ajutorul căruia se culeg date și informații despre utilizatorul calculatorului pe care rulează și se urmărește activitatea acestuia fără ca el să știe.

**Trol** – persoană care postează on-line comentarii aleatorii, în afara subiectului sau inflamatorii, cu scopul de a distrage atenția sau de a semăna discordie.

**White hat hacker** – hacker bine intenționat.

# CUPRINS

*Prefață* de Eugen Glăvan 5
*Notă asupra ediției în limba română* 9

Capitolul 1 – *Parazit* 15
Capitolul 2 – *Bulletproof* ..... 31
Capitolul 3 – *Războiul farma* ..... 59
Capitolul 4 – *Să-i cunoaștem pe cumpărători* 77
Capitolul 5 – *Ruleta rusească* 93
Capitolul 6 – *Partener în crima (dez)organizată* 119
Capitolul 7 – *Să-i cunoaștem pe spammeri* 137
Capitolul 8 – *Prieteni vechi, dușmani înverșunați* ..... 157
Capitolul 9 – *Întâlnire la Moscova* ..... 183
Capitolul 10 – *Antis* ..... 199
Capitolul 11 – *Închiderile* 219
Capitolul 12 – *Final de partidă* ..... 243
Epilog – *O lume fără spam. Cum ne putem proteja de criminalitatea informatică* ..... 263

*Mulțumiri* 273
*Surse* 275
*Glosar* 281

Pentru comenzi și informații, contactați:
**GRUPUL EDITORIAL CORINT**

**Departamentul de Vânzări**
Str. Mihai Eminescu nr. 54A, sector 1, București, cod poștal 010517
Tel./Fax: 021.319.47.97; 021.319.48.20

**Depozit**
Calea Plevnei nr. 145, sector 6, București, cod poștal 060012
Tel.: 021.310.15.30
E-mail: vanzari@edituracorint.ro
Magazin virtual: www.edituracorint.ro

Format: 16/54x84;
Coli tipo: 18

Tiparul executat la:

**Brian Krebs**
(n. 1972) este editorul blogului KrebsOnSecurity.com, dedicat informaţiilor de ultimă oră şi investigaţiilor din lumea securităţii informatice. În 2013, acesta a fost votat, pentru al treilea an consecutiv, „blogul care reprezintă cel mai bine industria securităţii informatice" de către juriul Conferinţei RSA, cea mai mare reuniune mondială din acest domeniu. KrebsOnSecurity a primit, de asemenea, premiul pentru cel mai instructiv blog de securitate informatică în 2013 şi 2014, iar în 2013 Krebs a fost inclus în Hall of Fame al autorilor de bloguri de specialitate, împreună cu expertul în securitate Bruce Schneier.

Ce putem face pentru a ne proteja de acest val distrugător de criminalitate informatică?

În *Națiunea Spam*, jurnalistul de investigație și expertul în securitate cibernetică Brian Krebs îi demască pe infractorii aflați la originea unora dintre cele mai ample campanii de spam care i-au vizat pe americani și conturile bancare ale acestora. Urmărind ascensiunea, căderea și alarmanta renaștere a mafiei digitale din spatele a două rețele de farmacii a căror existență se baza pe spam – și a nenumărați viruși, atacuri de phishing și malware – autorul ne propune prima lucrare definitorie privind spamul și riscurile pe care acesta le prezintă pentru utilizatorii de pretutindeni.

„Fascinantă! Cititorii nu se vor mai uita niciodată la mesajele nesolicitate cu aceiași ochi ca în trecut."

USA Today

Partener media

CITIT DE RADIO GUERRILLA

Carte recomandată de

Discovery CHANNEL

ISBN: 978-606-793-602-5

www.edituracorint.ro

CORINT FUTURE